

## Załącznik nr 9 do SIWZ

# OPIS PRZEDMIOTU ZAMÓWIENIA

w postępowaniu pn.:

**Dostawę wraz z montażem, uruchomieniem, konfiguracją i testami aktywnych urządzeń sieciowych w projekcie Pomorskie e-Zdrowie.**

---

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

## Spis treści

Spis treści.....	2
1. Słownik.....	6
2. Ogólny opis Przedmiotu Zamówienia .....	6
2.1 Cele projektu Pomorskie e-Zdrowie .....	6
2.2 Wykaz podmiotów biorących udział w realizacji Projektu.....	9
3. Przedmiot Zamówienia .....	10
4. Organizacja wdrożenia .....	11
4.1 Założenia podstawowe .....	11
4.2 Wymagania wdrożeniowe PZ.....	13
4.3 Harmonogram Wdrożenia (Harmonogram) .....	14
4.4 Wymagania dla Dokumentacji PZ .....	15
4.5 Wymagania funkcjonalne .....	16
4.5.1 Obszar sieci LAN.....	16
4.5.2 Obszar sieci WLAN .....	17
4.5.3 Obszar Oprogramowania Zarządzającego .....	18
4.6 Pozostałe wymagania techniczne i środowiskowe .....	19
4.7 Dostawa Przedmiotu Zamówienia .....	20
4.8 Instalacja i Wdrożenie.....	20
4.9 Procedura testowania.....	21
4.10 Procedury odbiorowe .....	22
4.11 Dokumentacja powykonawcza .....	22
4.12 Instruktaże stanowiskowe .....	22
4.13 Szkolenia specjalistyczne .....	24
4.14 Inne zobowiązania Wykonawcy.....	34
5. Opis specyficznych wymagań dla poszczególnych Podmiotów Leczniczych.....	35
5.1 PL01 - Wojewódzki Szpital Psychiatryczny im. prof. Tadeusza Bilikiewicza w Gdańsku .....	35
5.1.1 Ilość i rodzaj urządzeń.....	35

5.1.2	Wymagania konfiguracyjne. ....	35
5.2	PL02 - Stacja Pogotowia Ratunkowego w Gdańsku .....	36
5.2.1	Ilość i rodzaj urządzeń.....	36
5.2.2	Wymagania konfiguracyjne. ....	36
5.3	PL05 - Pomorskie Centrum Reumatologiczne im. dr Jadwigi Titz-Kosko w Sopocie Sp. z o.o. 37	
5.3.1	Ilość i rodzaj urządzeń.....	37
5.3.2	Wymagania konfiguracyjne. ....	37
5.4	PL06 Centrum Zdrowia Psychicznego w Słupsku .....	39
5.4.1	Ilość i rodzaj urządzeń.....	39
5.4.2	Wymagania konfiguracyjne. ....	39
5.5	PL07 Wojewódzki Szpital Specjalistyczny im. Janusza Korczaka w Słupsku Sp. z o.o. ....	40
5.5.1	Ilość i rodzaj urządzeń.....	40
5.5.2	Wymagania konfiguracyjne. ....	40
5.6	PL08 Szpital dla Nerwowo i Psychicznie Chorych im. St. Kryzana w Starogardzie Gdańskim	41
5.6.1	Ilość i rodzaj urządzeń.....	41
5.6.2	Wymagania konfiguracyjne. ....	41
5.7	PL10 Wojewódzki Ośrodek Terapii Uzależnień w Gdańsku .....	42
5.7.1	Ilość i rodzaj urządzeń.....	42
5.7.2	Wymagania konfiguracyjne. ....	42
5.8	PL11 Stacja Pogotowia Ratunkowego w Słupsku.....	43
5.8.1	Ilość i rodzaj urządzeń.....	43
5.8.2	Wymagania konfiguracyjne. ....	43
5.9	PL12.1 COPERNICUS PL Sp. z o.o.....	44
5.9.1	Ilość i rodzaj urządzeń.....	44
5.9.2	Wymagania konfiguracyjne. ....	44
5.10	PL14 Szpital Dziecięcy Polanki im. Macieja Płażyńskiego w Gdańsku Sp. z o.o. ....	47
5.10.1	Ilość i rodzaj urządzeń.....	47
5.10.2	Wymagania konfiguracyjne. ....	47

5.11	PL16 Szpital Specjalistyczny w Prabutach Sp. z o.o.....	48
5.11.1	Ilość i rodzaj urządzeń.....	48
5.11.2	Wymagania konfiguracyjne. ....	48
5.12	PL17 Przemysłowy Zespół Opieki Zdrowotnej Sp. z o.o.....	49
5.12.1	Ilość i rodzaj urządzeń.....	49
5.12.2	Wymagania konfiguracyjne. ....	49
5.13	PL18 Szpital Specjalistyczny w Kościerzynie Sp. z o.o. ....	50
5.13.1	Ilość i rodzaj urządzeń.....	50
5.13.2	Wymagania konfiguracyjne. ....	50
5.14	PL19.2 Szpitale Pomorskie Sp. z o.o.....	52
5.14.1	Ilość i rodzaj urządzeń.....	52
5.14.2	Wymagania konfiguracyjne. ....	52
6.	Specyfikacja ilościowa urządzeń aktywnych dla wszystkich PL.....	56
6.1	Sieć WLAN - urządzenia aktywne.....	56
6.2	Sieć przewodowa - urządzenia aktywne.....	56
7.	Specyfikacja techniczna Oprogramowania Zarządzającego (OZ).....	58
7.1	Podstawowe założenia dotyczące Oprogramowania Zarządzającego.....	58
7.2	Wymagania techniczne Oprogramowania Zarządzającego. ....	59
8.	Specyfikacja techniczna urządzeń aktywnych.....	63
8.1	Wymagania ogólne .....	63
8.2	Ogólne wymagania, wspólne dla wszystkich typów przełączników (punkty od 8.3 do 8.9) .	65
8.3	Przełącznik Access LAN PoE 24/10G .....	66
8.4	Przełącznik Access LAN PoE 48/10G .....	67
8.5	Przełącznik Access LAN 24G/10G.....	68
8.6	Przełącznik Access LAN 48G/10G.....	69
8.7	Przełącznik Access LAN 8G PoE.....	70
8.8	Przełącznik Core .....	71
8.9	Przełącznik serwerowy.....	73
8.10	Firewall w HA i licencje UTM – wspólne dla wszystkich typów firewall .....	75

---

8.11	Firewall w HA i licencji UTM – Typ A.....	84
8.12	Firewall w HA i licencji UTM – Typ B.....	85
8.13	Kontroler sieci bezprzewodowej – wymagania wspólne dla Typów A, B i C.....	86
8.14	Kontroler sieci bezprzewodowej TYP A.....	89
8.15	Kontroler sieci bezprzewodowej TYP B.....	90
8.16	Kontroler sieci bezprzewodowej Typ C.....	91
8.17	Access Point .....	92

## 1. Słownik

Słownik pojęć zawarty jest w Załączniku 10

## 2. Ogólny opis Przedmiotu Zamówienia

Projekt Pomorskie e-Zdrowie obejmuje 14 Podmiotów Leczniczych funkcjonujących na terenie Województwa Pomorskiego, dla których organem założycielskim jest SWP.

### 2.1 Cele projektu Pomorskie e-Zdrowie<sup>1</sup>

Celem głównym Projektu „Pomorskie e-Zdrowie” jest poprawa jakości i dostępności usług medycznych świadczonych na obszarze Województwa Pomorskiego oraz poprawa efektywności Podmiotów Leczniczych, dla których Województwo Pomorskie jest organem tworzącym.

Na poprawę jakości świadczeń zdrowotnych na poziomie regionalnym, a następnie ogólnokrajowym ma wpłynąć obowiązek prowadzenia przez PL dokumentacji medycznej w wersji elektronicznej. Konieczność prowadzenia dokumentacji medycznej tylko w postaci elektronicznej wymusza ustawa o systemie informacji w ochronie zdrowia. Jednakże warunkiem niezbędnym do spełnienia przez świadczeniodawców wymogów ustawy o systemie informacji w ochronie zdrowia, a zwłaszcza zapewnienia możliwości wymiany danych, w tym danych obrazowych oraz dokumentacji medycznej w postaci elektronicznej jest posiadanie przez nich m.in.: urządzeń diagnostycznych z cyfrowym zapisem wyników badań, łącz internetowych o odpowiedniej przepustowości, możliwości zapewnienia podmiotom trzecim dostępu do zgromadzonych danych medycznych oraz zdolność do ich pobierania z zasobów innych jednostek, w tym z zasobów CSIOZ.

System PeZ będzie systemem interoperacyjnym otwartym na współpracę z innymi systemami na poziomie regionalnym i krajowym (np. P1, P2 i P4).

W ramach Projektu zakłada się utworzenie portalu internetowego dla obywatela, informującego o pełnej ofercie pomorskiej ochrony zdrowia z możliwością zdalnej rejestracji pacjentów na wizyty do lekarza lub na inne świadczenia dostępne w Podmiotach Leczniczych oraz będącego źródłem wiedzy dotyczącej jakości leczenia w poszczególnych Podmiotach Leczniczych.

Realizacja planowanych w Projekcie działań doprowadzi do niezbędnego ucyfrowienia działalności podmiotów medycznych uczestniczących w Projekcie oraz zapewni interoperacyjność funkcjonujących

---

<sup>1</sup>Źródło: *Studium Wykonalności Projektu Pomorskie e-Zdrowie*

w nich systemów teleinformatycznych, co umożliwi komunikację z systemami e-zdrowia funkcjonującymi na poziomie krajowym.

W ramach realizacji Projektu powstaną lub zostaną rozbudowane istniejące interoperacyjne systemy dziedzinowe mające istotny wpływ na pracę Podmiotu Leczniczego m.in.:

- Systemy HIS (*ang. Hospital Information System*), mający uniwersalne zastosowanie w pracy personelu medycznego, w szczególności niezbędny do rozliczeń z NFZ i zasilania danymi elektronicznej dokumentacji medycznej wymaganej ustawą o systemie informacji w ochronie zdrowia,
- Systemy RIS i PACS (*ang. Radiology Information System i Picture Archiving and Communication System*) do archiwizacji wyników diagnostyki radiologicznej i transmisji obrazów cyfrowych,
- Systemy ERP (*ang. Enterprise Resource Planning*), czyli system wspomagania zarządzania zasobami przedsiębiorstwa, obejmujący takie obszary działalności jak: finanse i księgowość, kadry i płace, sprzedaż usług, gospodarkę magazynową itp.

Ucyfrowienie działalności PL wpłynie korzystnie na poprawę ich zdolności do wymaganej prawem, wieloletniej (nawet 25-50 lat) archiwizacji elektronicznej dokumentacji medycznej oraz usprawni zarządzanie danymi pacjentów w ramach wymogów stawianych przez RODO.

Cele pośrednie projektu obejmują:

1. Stworzenie pakietów usług elektronicznych z zakresu e-Zdrowia dla mieszkańców Województwa Pomorskiego.

Realizacja tego celu usprawni proces komunikacji pomiędzy pacjentami a Podmiotami Leczniczymi, intensyfikując możliwości przekazywania informacji przy jednoczesnym ograniczeniu czasochłonności procedur rejestracyjnych. Dzięki realizacji Projektu pacjenci otrzymają dostęp do:

- swojej dokumentacji medycznej zawierającej odbyte wizyty, wystawione recepty, opisy badań itp.
- danych krytycznych obejmujących podstawowe dane medyczne takie jak grupa krwi, waga, uczulenia i inne,
- danych na temat potrzeby odbycia niezbędnych badań, w tym profilaktycznych,
- edycji swoich podstawowych danych, w tym danych kontaktowych.

2. Stworzenie pakietów usług elektronicznych dla Podmiotów Lecznicznych.

Realizacja tego celu stworzy możliwość PL:

- wytwarzania, przetwarzania, wymiany i archiwizacji dokumentacji medycznej świadczeniobiorców,
- wsparcia procesów związanych z realizacją procesów leczenia.

Realizacja celu usprawni obieg dokumentów w Podmiotach Leczniczych, pozwoli na szybki i bezpieczny dostęp do dokumentów medycznych pacjenta nawet jeżeli był on leczony w innej placówce. W efekcie uzyskana zostanie częściowa optymalizacja kosztów badań, które nie będą powtarzane w każdej jednostce, do której zgłosi się pacjent. PeZ udostępniając bieżącą informację o dostępności usług medycznych oraz specjalistów pozwoli na sprawniejsze zarządzanie placówkami i efektywniejsze wykorzystanie posiadanych zasobów.

3. Stworzenie pakietu usług elektronicznych dla WP.

Pakiet usług elektronicznych dla WP to zestaw narzędzi i funkcjonalności wspierających Podmioty Lecznicze w zarządzaniu danymi i dokumentacją medyczną, ułatwiających zarządzanie nimi, a także gwarantujących poprawę jakości nadzoru właścicielskiego.

PeZ umożliwi WP dostęp do informacji zarządczej (wglądu do raportów i prezentacji na temat działań Podmiotów Leczniczych) oraz umożliwi nadzór nad systemami obsługi jakości i zdarzeń niepożądanych.

4. Podniesienie poziomu informatyzacji poszczególnych PL.

Realizacja tego celu ma zapewnić odpowiednią infrastrukturę informatyczną umożliwiającą funkcjonowanie PeZ. Realizacja tego celu polega na dostosowaniu pomieszczeń pod serwerownie, zakupu stacji roboczych, platform dostępowych i serwerowych oraz rozbudowie infrastruktury sieciowej. Realizacja tego celu podniesie poziom informatyzacji poszczególnych placówek, a jednocześnie umożliwi działanie systemu na skalę regionalną.

5. Zapewnienie interoperacyjności systemów informatycznych w ochronie zdrowia.

Realizacja tego celu ma zapewnić kompleksową integrację systemów ochrony zdrowia, zarówno w wymiarze regionalnym jak i ogólnopolskim – systemy krajowe to m.in. Platforma P1 (Elektroniczna Platforma Gromadzenia i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych), Platforma P2 (Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych), Platforma P4 (Dziedziczne systemy teleinformatyczne systemu informacji w ochronie zdrowia).



## 2.2 Wykaz podmiotów biorących udział w realizacji Projektu

Tabela 1 Wykaz podmiotów biorących udział w realizacji Projektu

Lp.	Identyfikator Podmiotu Leczniczego	Pełna nazwa Podmiotu Leczniczego
1.	PL01	Wojewódzki Szpital Psychiatryczny im. prof. Tadeusza Bilikiewicza w Gdańsku
2.	PL02	Stacja Pogotowia Ratunkowego w Gdańsku
3.	PL05	Pomorskie Centrum Reumatologiczne im. dr Jadwigi Titz-Kosko w Sopocie Sp. z o.o.
4.	PL06	Centrum Zdrowia Psychicznego w Słupsku
5.	PL07	Wojewódzki Szpital Specjalistyczny im. Janusza Korczaka w Słupsku Sp. z o.o.
6.	PL08	Szpital dla Nerwowo i Psychiczenie Chorych im. St. Kryzana w Starogardzie Gdańskim
7.	PL10	Wojewódzki Ośrodek Terapii Uzależnień w Gdańsku
8.	PL11	Stacja Pogotowia Ratunkowego w Słupsku
9.	PL12.1	COPERNICUS PL Sp. z o.o.
10.	PL14	Szpital Dziecięcy Polanki im. Macieja Płażyńskiego w Gdańsku Sp. z o.o.
11.	PL16	Szpital Specjalistyczny w Prabutach Sp. z o.o.
12.	PL17	Przemysłowy Zespół Opieki Zdrowotnej Sp. z o.o.
13.	PL18	Szpital Specjalistyczny w Kościerzynie Sp. z o.o.
14.	PL19.2	Szpital Pomorskie Sp. z o.o.

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

### 3. Przedmiot Zamówienia

Przedmiot zamówienia obejmuje:

- Opracowanie Harmonogramu i Dokumentacji Projektowej (DPR),
- Dostarczenie wszystkich komponentów sprzętowych i oprogramowania,
- Montaż, podłączenie, konfiguracja, uruchomienie i wdrożenie wszystkich dostarczonych komponentów zgodnie z ilością przypisaną dla PL,
- Dostarczenie i podłączenie niezbędnego okablowania oraz innego niezbędnych akcesoriów (np. wkładek) dla urządzeń dostarczanych w ramach PZ oraz zasilania w infrastrukturze PL,
- Niezbędną konfigurację środowiska LAN, WAN i WLAN Zamawiającego,
- Wykonanie i dostarczenie Dokumentacji Powykonawczej DPO i Dokumentacji Użytkowej (DU),
- Przeprowadzenie instruktaży stanowiskowych w zakresie merytorycznym niezbędnym do instalacji, konfiguracji i użytkowania PZ,
- Przeprowadzenie Szkoleń specjalistycznych,
- Świadczenie Usługi Serwisowej (US) i Gwarancji Wykonawcy (GW) w trakcie całego okresu gwarancji.

---

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

## 4. Organizacja wdrożenia

### 4.1 Założenia podstawowe

- 1) Wykonawca umożliwi Zamawiającemu udział we wszystkich pracach realizowanych w ramach PZ (m.in. w czasie projektowania, dostawach, instalacji, konfiguracji i wdrożeniu).
- 2) Wykonawca zobowiązany jest przeprowadzić dostawy PZ w terminach i godzinach uzgodnionych z Zamawiającym z minimum 5 dniowym wyprzedzeniem.
- 3) Infrastruktura sieciowa musi być oznakowana w taki sposób, aby możliwa była identyfikacja systemowa zarówno produktu, numeru seryjnego, daty produkcji (dopuszczalna informacja w systemie urządzenia) jak i producenta (z wyłączeniem przewodów zasilających i sygnałowych).
- 4) Infrastruktura sieciowa musi być dostarczona Zamawiającemu w oryginalnych opakowaniach fabrycznych w celu weryfikacji jej pochodzenia. Zamawiający dopuszcza otworenie opakowań przed dostawą w celu wykonania wstępnej konfiguracji/aktualizacji oprogramowania.
- 5) Oferowane urządzenia muszą być fabrycznie nowe (wcześniej nieużywana) i pochodzić z autoryzowanego kanału dystrybucji producenta w Polsce (niedopuszczalne jest dostarczanie sprzętu z kanałów brokerskich).
- 6) Wszystkie urządzenia muszą posiadać oznakowanie CE.
- 7) Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia urządzenia w EOL (brak wsparcia producenta lub wycofanie urządzenia z oficjalnej dystrybucji).
- 8) Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V ± 10%, 50 Hz. (chyba, że w wymaganiach szczegółowych jest wyspecyfikowane inaczej)
- 9) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim. Nie dopuszcza się dokumentacji w język angielskim w przypadku dostępności dokumentacji w języku polskim.
- 10) Do każdego urządzenia musi być dostarczony niezbędny osprzęt eksploatacyjny (przewody zasilające, przewody sygnałowe itp.) niezbędny do uruchomienia danego urządzenia w budowanym rozwiązaniu w miejscu instalacji wskazanym przez Zamawiającego. Osprzęt, o którym mowa powyżej jest integralną częścią oferty i przechodzi na własność Zamawiającego.
- 11) Wykonawca jest zobowiązany do doboru odpowiednich, do przewidywanych odległości pomiędzy poszczególnymi urządzeniami oraz istniejącym w projektowanym miejscu połączeniami, typów wkładek do interfejsów komunikacyjnych.
- 12) Wszystkie odpady związane z dostawami i realizacją przedmiotu zamówienia Wykonawca usunie na własny koszt, poza terenem Zamawiającego, zgodnie z przepisami obowiązującymi na terenie Rzeczypospolitej Polski.

- 13) Dostarczane oprogramowanie musi zostać dostarczonej w najnowszej stabilnej wersji, która uzyskała certyfikację producenta dostarczanego sprzętu (jeśli podlega certyfikacji). Na pisemny wniosek Zamawiającego wersja ta może zostać zmieniona do wersji starszej niż aktualnie dostępna (jeśli istnieje taka możliwość).
- 14) Urządzenia muszą być przystosowane do montażu w szafie 19" – tzn. posiadać wszystkie niezbędne uchwyty i mocowania z osprzętem.
- 15) Przez Wdrożenie należy rozumieć szereg uporządkowanych i zorganizowanych działań mających na celu wykonanie PZ.
- 16) Wdrożenie PZ będzie realizowane w ramach powołanych do tego celu struktur organizacyjnych po stronie Wykonawcy.
- 17) W ramach Wdrożenia Wykonawca przygotowuje i przekazuje informacje na temat struktury organizacyjnej Zespołu Projektowego Wykonawcy, w ramach której muszą zostać powołane minimum następujące role w projekcie:
  - a) Kierownik Projektu ze strony Wykonawcy,
  - b) Koordynator ds. Wdrożenia ze strony Wykonawcy.
- 18) Wdrożenie, muszą realizować osoby wymienione w ofercie Wykonawcy, przy czym:
  - a) Prace instalacyjne, konfiguracyjne i wdrożeniowe muszą być przeprowadzane przez osoby posiadające stosowne uprawnienia i doświadczenie w zakresie, objętym PZ,
  - b) Osoby Zespołu Projektowego Wykonawcy muszą być dyspozycyjne w trakcie wykonywania robót instalacyjnych i wdrożeniowych,
  - c) Wykonawca przekazuje Zamawiającym wykaz numerów telefonów kontaktowych i adresów email do osób biorących udział w realizacji PZ po stronie Wykonawcy oraz godziny pracy pracowników,
  - d) Zamawiający wymaga, by wszelkie zastępstwa lub trwała zmiana w zespole osób ze strony Wykonawcy były niezwłocznie zgłaszane przez Wykonawcę, z zastrzeżeniem, że osoba zastępująca musi posiadać nie mniejsze kwalifikacje niż osoba zastępowana,
  - e) Zastępstwo lub trwała zmiana danej osoby nie wymaga akceptacji ze strony Zamawiających, chyba, że Wykonawca nie spełni zastrzeżenia w ustępie poprzednim
  - f) Zamawiający w uzasadnionych przypadkach, ma prawo zażądać zmiany osoby będącego w zespole Wykonawcy podając merytoryczne uzasadnienie takiej decyzji.
- 19) Prace należy zorganizować tak, aby Zamawiający w minimalnym stopniu byli pozbawieni dostępu do systemów i usług teleinformatycznych. Wszelkie konieczne przerwy wymagają uzgodnienia z Zamawiającym i wymagają jego zgody.
- 20) Obiekty podlegające inwestycji (obiekty Służby Zdrowia w których świadczone są usługi medyczne) są użytkowane w trybie ciągłym w czasie godzin pracy przez cały okres wykonywania PZ, co może powodować utrudnienia w miejscu prowadzenia prac. Nie ma możliwości całkowitego wyłączenia i zamknięcia ww. obiektów na czas realizacji PZ. W przypadku wystąpienia konieczności przeprowadzenia prac brudnych lub głośnych podczas instalacji urządzeń, poszczególne

pomieszczenia będą przekazywane etapami, tak aby zachować ciągłość świadczenia usług medycznych zgodnie z harmonogramem uzgodnionym z Zamawiającym.

- 21) Wykonawca musi przewidzieć i zagwarantować odpowiednie zabezpieczenia miejsc wykonywania poszczególnych elementów dostawy z uwagi na fakt, że wszystkie prace wykonywane będą w użytkowanym obiekcie przy dużym ruchu pracowników i chorych, tzn. organizacja prac musi przede wszystkim zapewniać bezpieczeństwo przebywających w oddziale pracowników i chorych oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiających.
- 22) Wykonawca w trakcie analizy musi przewidzieć i uwzględnić konieczność rekonfiguracji ustawień sieciowych urządzeń medycznych. Wykonanie rekonfiguracji zgodnie z wytycznymi Wykonawcy leży w zakresie Zamawiającego.
- 23) Odpowiedzialność za dostarczony i zamontowany sprzęt, do momentu podpisania stosownego protokołu odbioru, spoczywa na Wykonawcy.
- 24) Wykonawca zobowiązany będzie do zapoznania się i przestrzegania Polityki Bezpieczeństwa i zasad przetwarzania danych osobowych stosowanych w każdym PL oraz podpisania stosownych oświadczeń i ewentualnych umów powierzenia przetwarzania danych.

## 4.2 Wymagania wdrożeniowe PZ

Zamawiający wymaga aby proces wdrożenia Urządzeń aktywnych Infrastruktury sieciowej był prowadzony zgodnie z zaplanowanym Harmonogramem i w ramach zaplanowanego budżetu. Wykonawca realizujący wdrożenie musi zatem stosować wielokrotnie sprawdzoną metodykę. Jej skuteczność potwierdzona musi być wieloletnim doświadczeniem nabytym podczas realizacji wielu udanych wdrożeń. Metodyka ta musi opierać się na ścisłej współpracy z przedstawicielami Zamawiającego, w szczególności uwzględniając czynne włączenie w proces wdrożenia przyszłych użytkowników Administratorów systemu. Takie podejście do problematyki wdrożenia zmniejsza bowiem ryzyko niepowodzenia i ogranicza budżet przedsięwzięcia.

Właściwe prowadzenie i zarządzanie dużym projektem informatycznym ma kluczowe znaczenie dla powodzenia projektu – uruchomienia Infrastruktury sieciowej w zaplanowanym zakresie, terminie i budżecie. Dlatego Zamawiający wymaga, wykonania prac przez Wykonawcę zgodnie z jedną z uznanych metodyk zarządzania projektami.

### 4.3 Harmonogram Wdrożenia (Harmonogram)

- 1) Przedmiot Zamówienia będzie realizowany w oparciu o przygotowany uprzednio przez Wykonawcę Harmonogram Wdrożenia dla każdego PL z osobna w oparciu o Harmonogram Projektu umieszczony w Tabeli 2. Harmonogram ten musi być uzgadniany i zaakceptowany każdorazowo przez Zamawiającego oraz systematycznie aktualizowany i utrzymywany przez Wykonawcę w toku realizacji PZ. Harmonogram Projektu wyznacza nieprzekraczalne terminy wykonania danego Etapu realizacji. Przygotowany przez Wykonawcę Harmonogram Wdrożenia może przewidywać realizację danego Etapu w terminie krótszym niż zakłada Harmonogram Projektu.
- 2) Wykonawca w Harmonogramie Wdrożenia musi uwzględnić podział na zadania, w szczególności: projektowanie i dostawy oraz instalacja, konfiguracja, testowanie, wdrożenie, odbiory oraz dostarczenie Dokumentacji Przedmiotu Zamówienia wraz z planowaną datą odbioru końcowego.

Tabela 2 Podstawowe etapy i terminy realizacji – Harmonogram Projektu

ETAP	OPIS	TERMIN WYKONANIA
I.	<b>Projektowanie</b> Uzgodnienie i opracowanie Dokumentacji Projektowej (DPR) niezbędnej do wykonania PZ ze szczegółowym Harmonogramem Wdrożenia	Do 90 dni od daty podpisania Umowy
II.	<b>Dostawa komponentów</b> Dostawy wszystkich kompletnych komponentów i produktów	Do 180 dni od daty podpisania Umowy
III.	<b>Instalacja, konfiguracja i wdrożenie komponentów, przeprowadzenie Szkoleń specjalistycznych</b> Wykonanie całości instalacji, konfiguracja i wdrożenie zgodnie z Dokumentacją oraz przeprowadzenie Szkoleń Specjalistycznych.	Do 300 dni od daty podpisania Umowy
IV.	<b>Opracowanie Dokumentacji Powykonawczej i Dokumentacji Użytkowej</b> <b>Odbiory</b> Wykonanie Dokumentacji powykonawczej (DPO) i Dokumentacji Użytkowej (DU) oraz dostarczenie pozostałej niezbędnej dokumentacji (np. potwierdzeń objęcia gwarancją producenta dostarczonych urządzeń). <i>(Dokumentacja powykonawcza musi zawierać szczegółowa konfigurację każdego z dostarczonych urządzeń lub Wykonawca musi dostarczyć oprogramowanie wraz z licencją, która umożliwi w czasie rzeczywistym odczytać zapisaną w urządzeniu konfigurację i zrobić z niej kopię zapasową).</i>	Do 330 dni od daty podpisania Umowy

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

ETAP	OPIS	TERMIN WYKONANIA
	Testy funkcjonalne. Odbiory poszczególnych Komponentów Odbiór końcowy	

#### 4.4 Wymagania dla Dokumentacji PZ

1. W początkowym stadium realizacji PZ (Etap I) Wykonawca opracuje Dokumentację Projektową i uzgodni ją z Zamawiającymi. Zamawiający ma każdorazowo ilość dni zgodnych z Umową na odpowiedź (akceptację lub precyzyjne uwagi) na przesłane w formie pisemne (papierowej lub elektronicznej) uzgodnienia bądź pytania. Istnieje możliwość uzgodnienia dłuższego terminu odpowiedzi w uzgodnieniu z Wykonawcą.
2. DP będzie stanowić bazowe zapisy opisujące sposób realizacji PZ. Na podstawie zapisów w tej dokumentacji oraz pozostałych zapisów SIWZ będzie realizowany, a następnie odbierany PZ.
3. W kolejnych Etapach Wykonawca opracuje w porozumieniu z Zamawiającymi pozostałą dokumentację, która obejmie:
  - a. DPO,
  - b. DU.
4. Dokumentacja wraz z SIWZ będą stanowiły podstawę do weryfikacji funkcjonalnej i jakościowej w trakcie odbiorów PZ.
5. Dokumentacja podlega uzgadnianiu i akceptacji Zamawiających. Akceptacja Dokumentacji Projektowej warunkuje rozpoczęcie prac Wykonawcy. Zamawiający ma każdorazowo ilość dni zgodnych z Umową na odpowiedź (akceptację lub precyzyjne uwagi) na przesłane w formie pisemne (papierowej lub elektronicznej) uzgodnienia bądź pytania. Istnieje możliwość uzgodnienia dłuższego terminu odpowiedzi w uzgodnieniu z Wykonawcą.
6. W związku z tym, że zamówienie realizowane jest w ramach Projektu współfinansowanego przez Unię Europejską z Europejskiego Funduszu Rozwoju Regionalnego oraz budżetu Państwa w ramach Regionalnego Programu Operacyjnego Województwa Pomorskiego na lata 2014 – 2020, Wykonawca zobowiązuje się do umieszczania odpowiednich oznaczeń i logotypów zgodnych z Wytycznymi Instytucji Zarządzającej tym programem w zakresie informacji i promocji na Dokumentacji, Komponentach i Produktach wytwarzanych/dostarczanych w wyniku realizacji PZ.

## 4.5 Wymagania funkcjonalne

- 1) Celem budowy Infrastruktury sieciowej w PL jest przygotowanie wydajnej i bezpiecznej platformy sprzętowo-programowej dla obsługi ruchu sieciowego pochodzącego zarówno od użytkowników zewnętrznych i wewnętrznych w użytkowaniu systemów informatycznych. Musi ona być zbudowana zgodnie z najlepszymi praktykami w zakresie projektowania i zabezpieczania tego typu systemów oraz uwzględniać zapas wydajności na przyszłe potrzeby związane z pozostałą wdrażaną infrastrukturą teleinformatyczną Zamawiającego w ramach projektu PeZ.
- 2) Docelowa architektura fizyczna i logiczna sieci Zamawiającego musi składać się z dostarczanych elementów Infrastruktury sieciowej, elementów istniejących oraz umożliwić prawidłowe i efektywne działanie sieci teleinformatycznej każdego PL.
- 3) Wszystkie działania Wykonawcy podczas Etapów muszą zostać przeprowadzone zgodnie z Harmonogramem Wdrożenia i zakończone pozytywnym wynikiem testów oraz odbiorem.
- 4) Zamawiający ma prawo do odstąpienia od poniższych wymogów, ich zmiany lub zaproponowania nowych w uzgodnieniu z Wykonawcą na etapie opracowania DPR.
- 5) Wykonawca w ramach przygotowania DPR, a następnie podczas wdrożenia dla każdego PL musi zaprojektować i wdrożyć architekturę sieci, która musi zapewnić wydzielenie odpowiednich stref bezpieczeństwa dostosowanych do aplikacji i usług uruchomionych w danej strefie.

### 4.5.1 Obszar sieci LAN

- 1) Wykonawca musi wykonać co najmniej następujące czynności:
  - a) Strefy bezpieczeństwa muszą zostać zaprojektowane i wykonane z wykorzystaniem urządzeń klasy firewall i/lub UTM.
  - b) Muszą być wydzielone co najmniej następujące strefy bezpieczeństwa (strefy mogą być różne w zależności od wymogów poszczególnych Zamawiających): (wymóg ten może ulec zmianie jeśli zażyczy sobie tego dana placówka)
    - (1) DMZ (strefa ograniczonego zaufania, w której umieszczone są usługi dla zewnętrznych użytkowników, np. serwer WWW lub poczta elektroniczna; serwery w tej strefie nie posiadają dostępu do sieci wewnętrznej, w której uruchomione będą systemy dziedziczone,
    - (2) Strefa chroniona (ang. Secured Zone) – strefa chroniona w wysokim stopniu przez zastosowanie mechanizmów kontroli na urządzeniach typu firewall; nie jest możliwy bezpośredni dostęp z sieci Internet do serwerów/aplikacji umieszczonych w tej strefie; dostęp możliwy jest tylko i wyłącznie dla zdefiniowanych hostów oraz usług; strefa ta przewidziana jest dla systemów dziedziczone,
    - (3) Strefy dla sieci WLAN,
    - (4) Stref wewnętrznych LAN dla pracowników PL.
- 2) Ponadto Wykonawca musi w sieciach wszystkich PL co najmniej :

---

### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE



- a) Zrealizować założenia zatwierdzone przez obie strony w DRP.
- b) Wdrożyć mechanizmy routingu pomiędzy wszystkimi strefami wraz z ustalonymi z Zamawiającym politykami bezpieczeństwa. Mogą być one przypisane na użytkownika (integracja z AD/LDAP).
- c) Zapewnić mechanizmy kontroli routingu w celu zapewnienia właściwego przepływu informacji zgodnie ze zdefiniowaną polityką kontroli dostępu do aplikacji np. systemy dziedzinowe; routing musi zostać zrealizowany w oparciu o weryfikację adresów źródłowych i docelowych.
- d) Wdrożyć odpowiednią konfigurację urządzeń sieciowych w celu ograniczenia dostępu do interfejsu administracyjnego dla ściśle określonej grupy administratorów.
- e) Wdrożyć mechanizmy i zasady dostępu do sieci wewnętrznej, który jest dozwolony wyłącznie dla pracowników i osób upoważnionych.
- f) U uruchomić mechanizmy pozwalające na skuteczne zapobieganie niepożądanym sytuacjom w krytycznych segmentach sieci (np. zapobieganie pętlom).
- g) U uruchomić mechanizm umożliwiający zarządzanie siecią i pozwalający na monitorowanie parametrów sieci w czasie rzeczywistym (min. snmp, syslog, ntp).
- h) Wdrożyć filtrację pomiędzy segmentami sieci poprzez dostarczone urządzenia.
- i) Wdrożyć mechanizmy zapewnienia jakości usług dla aplikacji krytycznych.

#### 4.5.2 Obszar sieci WLAN

- 1) Ze względu na specyfikę działania sieci bezprzewodowych wymagane jest:
  - a) Uruchomienie sieci bezprzewodowej w standardzie 802.11 ac.
  - b) Rozdzielenie segmentów sieci bezprzewodowych od segmentów sieci przewodowej wewnętrznej,
  - c) W PL gdzie nie były wykonywane pomiary przez wykonawcę części pasywnej Zamawiający dostarczy rzuty pomieszczeń i kondygnacji. Zamawiający nie gwarantuje dostępu do edytowalnych wersji cyfrowych niniejszych rzutów.
  - d) Wdrożenie scentralizowanego, redundantnego modelu zarządzania wszystkimi punktami dostępowymi sieci WLAN z zastosowaniem kontrolerów WLAN.
  - e) Uruchomienie na urządzeniach dedykowanych sieci (multi SSID) minimum dla: pracowników, gości, dla tabletów medycznych
  - f) Liczba SSID, nazwy, ich funkcjonalność oraz sposób implementacji Wykonawca uzgodni z każdym z PL i opíše w DPR.
  - g) Zapewnienie roamingu pomiędzy punktami dostępowymi dla urządzeń końcowych.
  - h) Uruchomienie bezpiecznych algorytmów szyfrowania i uwierzytelniania w sieci (wymagane jest wykorzystywanie przynajmniej algorytmu WPA2 PSK),
  - i) Autoryzację użytkowników w oparciu o protokół 802.1x dla segmentów sieci WLAN, gdzie pracownicy PL korzystają z dostępu do systemów medycznych (uwierzytelnianie pracowników w oparciu o konto i hasło z istniejących usług katalogowych). Element realizowany tylko

- w przypadku, gdy Zamawiający posiada wdrożoną i pracującą produkcyjnie usługę katalogową współpracującą z dostarczaną Infrastrukturą sieciową)
- j) Wdrożenie funkcjonalności portalu dla gości (Captive Portalu) z koniecznością potwierdzenia regulaminu oraz możliwością limitowania czasu i prędkości. Treść zapisu regulaminu dostarcza Zamawiający.
  - k) Przygotowanie mechanizmów QoS przydziału odpowiedniego pasma użytkownikowi poprzez mechanizmy wbudowane w dostarczone rozwiązanie.
  - l) Uruchomienie mechanizmów monitorowania obciążenia wydajności sieci WLAN na dostarczonych urządzeniach.
  - m) Przeprowadzenie pomiarów po instalacji i wdrożeniu sieci WLAN; Na ich podstawie przedstawienie raportu potwierdzającego pokrycie sygnałem i zapewnienie wymaganych parametrów oraz funkcjonalności sieci WLAN w PL.
  - n) Wdrożenie innych wymagań usług i mechanizmów specyficznych dla PL opisanych w pkt 5.

#### 4.5.3 Obszar Oprogramowania Zarządzającego

- 1) Wymagana jest konfiguracja Oprogramowania Zarządzającego w zakresie wszystkich dostarczanych w ramach postępowania przełączników, kontrolerów sieci bezprzewodowej i punktów dostępowych. Wymaga się co najmniej następujących czynności związanych z Oprogramowaniem Zarządzającym:
  - a) Instalacja Oprogramowania Zarządzającego na infrastrukturze serwerowej Zamawiającego. Dostarczenie niezbędnego oprogramowania systemowego (oprogramowanie bazowanego, system operacyjny) do poprawnego działania oprogramowania leży po stronie Wykonawcy. Wykonawca winien w takim przypadku dostarczyć licencje na w/w oprogramowanie, którego właścicielem i licencjobiorcą będzie Zamawiający.
  - b) Wstępna konfiguracja i optymalizacja Oprogramowania Zarządzającego
  - c) Aktywacja/rejestracja licencji jeśli wymagana
  - d) Podłączenie do Oprogramowania Zarządzającego wszystkich dostarczanych w ramach postępowania przełączników, kontrolerów sieci bezprzewodowej i punktów dostępowych
  - e) Konfiguracja w porozumieniu z Zamawiającym całej podłączonej do Oprogramowania Zarządzającego infrastruktury.
  - f) Konfiguracja alertów i raportów,
  - g) Stworzenie i implementacja polityki backupów konfiguracji urządzeń oraz ich odtwarzania z backupów przechowywanych w OZ
  - h) Konfiguracja mechanizmu przeglądania zdarzeń w sieci
  - i) Implementacja widoków dla administratora
  - j) Stworzenie w mapy sieci (złożonej z dostarczanych urządzeń) wraz z dynamiczną prezentacją zmian stanu tych urządzeń (stan przełącznika, portu)

- k) Implementacja mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym
- l) Implementacja list i zbierania informacji o kontrolerach WLAN, tworzenia list i zbierania informacji o punktach dostępowych WLAN
- m) Wgranie planu budynku (dostarczonego przez Zamawiającego w obsługiwanej formie) i rozmieszczenie na nim punktów dostępowych. W przypadku braku dostarczenia mapki przez Zamawiającego wymóg ten nie jest obligatoryjny.

#### 4.6 Pozostałe wymagania techniczne i środowiskowe

Wykonawca w ramach realizacji PZ dostarczy niezbędną Infrastrukturę sieciową i zrealizuje poniższe działania:

1. Dokona montażu fizycznego wszystkich dostarczonych komponentów i produktów w miejscu uzgodnionym z Zamawiającym.
2. Dostarczy wszystkie Urządzenia Aktywne z najnowszą - dostępną na termin dostawy - wersją oprogramowania (firmware). Na pisemny wniosek Zamawiającego wersja ta może zostać zmieniona do wersji starszej niż aktualnie dostępna (jeśli istnieje taka możliwość).
3. Podłączy dostarczaną Infrastrukturę sieciową do instalacji zasilającej Zamawiającego oraz dostarczy i podłączy okablowaniem LAN dostarczaną Infrastrukturę sprzętową do istniejącej infrastruktury Zamawiającego (jeśli konieczne). Zamawiający zapewni punkt styku z obecną infrastrukturą w danej lokalizacji. Wykonawca przygotuje fizyczny port w urządzeniu w celu podłączenia obecnej infrastruktury.
4. Zainstaluje przełączniki w każdym PPD, GPD i serwerowniach; przełączniki muszą być łączone i skonfigurowane w taki sposób, aby tworzyć pojedyncze urządzenie logiczne (tzw. Stack).
5. Podłączy przełączniki w PPD poprzez dwie drogi światłowodowe (w technologii światłowodowej dostępnej w danym PL jeśli możliwe) z węzłem nadrzędnym z wykorzystaniem redundantnych urządzeń pracujących w trybie failover w technologii 10G lub 1G (tam gdzie nie przewidziano urządzeń z interfejsami 10G i gdzie możliwe jest połączenie poprzez 2 drogi).
6. Obsługa zmultiplikowanych połączeń (protokołów agregujących zmultiplikowane połączenia) w sieci będzie odbywać się bez konieczności stosowania protokołu STP lub podobnych rozwiązań stwarzających potencjalne zagrożenia wystąpienia pętli w sieci.
7. Zastosuje architekturę dwuwarstwową sieci - przełączniki Core i przełączniki dostępowe zarówno w serwerowniach jak i do podłączenia komputerów w sieci.
8. Wszystkie przewody muszą zostać opisane etykietami w postaci tak zwanych flag na obu zakończeniach.

---

#### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

9. Głównym elementem sprzętowym pełniącym funkcję rdzenia sieci będą przełączniki Core; wymagana jest taka konfiguracja sieci, aby pełniły one rolę zarówno agregatorów połączeń z warstwy dostępowej, jak również dostarczały magistralę dla połączeń pomiędzy wszystkimi blokami funkcjonalnymi i kluczowymi segmentami sieci; obie pary przełączników muszą pracować w pełnej redundancji HA (active/active) (tam gdzie ilość urządzeń na to pozwala); dla umożliwienia skutecznego zarządzania przełączniki muszą być widziane przez system zarządzania jako pojedyncze logiczne urządzenie.
10. Zintegruje dostarczoną Infrastrukturę sieciową ze środowiskiem sieci LAN Zamawiającego w zakresie logicznej spójności. Wykonawca nie jest odpowiedzialny za rekonfigurację infrastruktury sieciowej tworzącej aktualne środowisko sieci LAN Zamawiającego. Przez integrację rozumie się wskazanie zaleceń konfiguracyjnych (które na istniejących urządzeniach wykona Zamawiający) na etapie DRP, które umożliwią wspólną pracę dostarczanej w ramach postępowania infrastruktury sprzętowej wraz z infrastrukturą obecną u Zamawiającego. Zamawiający zapewni punkt styku z obecną infrastrukturą w danej lokalizacji. Wykonawca przygotuje fizyczny port w urządzeniu w celu podłączenia obecnej infrastruktury.
11. Użyje jednoznacznego oznaczenia okablowania oraz sprzętu w celu uniknięcia błędów w podłączeniu dostarczonych komponentów i produktów. Poprzez oznaczenie rozumie umieszczenie flagi na każdym zakończeniu kabla oraz oznakowaniu każdego urządzenia w widocznym miejscu zarówno z przodu jak i z tyłu urządzenia. Oznakowanie musi być na tyle trwałe, aby wytrzymało warunki pomieszczeń technicznych typu serwerownia czy węzeł sieciowy.
12. Wszystkie elementy sprzętowe dostarczonej Infrastruktury sieciowej muszą być wyposażone w komplet akcesoriów niezbędnych do instalacji tak, aby po uruchomieniu osiągnęły wymaganą funkcjonalność.

#### 4.7 Dostawa Przedmiotu Zamówienia

1. Wykonawca w Etapie I przedstawi i uzgodni harmonogram dostaw dla poszczególnych PL.
2. Zamawiający dopuszcza w okresie trwania Umowy, możliwość dostawy Przedmiotu Zamówienia w częściach, po wcześniejszym uzgodnieniu z Zamawiającym i uzyskaniu jego zgody.
3. Do czasu odbioru PZ przez Zamawiającego ryzyko wszelkich niebezpieczeństw związanych z ewentualnym uszkodzeniem lub utratą sprzętu ponosi Wykonawca.

#### 4.8 Instalacja i Wdrożenie

1. W ramach Wdrożenia PZ Wykonawca dostarczy wszystkie niezbędne materiały pomocnicze dla Infrastruktury sieciowej takich jak:

- a) wkładki światłowodowe – wymagane jest dostarczenie wkładek dla wszystkich portów obsługujących wkładki światłowodowe w dostarczanej Infrastrukturze sieciowej. Dobór poszczególnych wkładek zostanie przeprowadzony w uzgodnieniu z Zamawiającym na etapie DPR. Dobór wkładek dotyczy także urządzeń Firewall. Zakłada się możliwość doboru wkładek o różnych przepustowościach (np. 1 Gbit, 10 Gbit) oraz o dowolnych parametrach obsługiwanych przez dostarczaną Infrastrukturę sieciową.
  - b) kable sygnałowe – wymagane jest dostarczenie wszystkich niezbędnych kabli sygnałowych (zarówno miedzianych jak i światłowodowych) wymaganych do uruchomienia dostarczanej Infrastruktury sieciowej w miejscu jej instalacji. Dodatkowo wymaga się dostarczenie ilości patchcordów miedzianych i światłowodowych w ilości pozwalającej do przekrosowania wszystkich gniazd w przełącznikach dostępowych dostarczanych w ramach postępowania. Długość i kolor zostaną dobrane w uzgodnieniu Zamawiającym na etapie DPR. Nie przewiduję się dostarczania patchcordów dłuższych niż 10m do przekrosowania przełączników.
  - c) kable zasilające, organizery, trwałe etykiety itp. wymagane do uzyskania opisanych funkcjonalności w SIWZ i DPR.
2. Dostarczone kable sygnałowe muszą mieć parametry nie gorsze niż parametry i klasa okablowania strukturalnego niskoprądowego dostarczonego przez Wykonawcę części pasywnej projektu PeZ (klasa nie niższa niż 6A).
  3. W ramach dostaw należy uwzględnić wszelkie niezbędne elementy sprzętowe, kablowe i oprogramowanie (licencje) w każdym PL i całym projekcie tak, aby Zamawiający otrzymał w pełni funkcjonalną i wartościową infrastrukturę, która będzie poprawnie i w całym zakresie funkcji współpracować ze wszystkimi zamawianymi elementami sieci aktywnej.

#### 4.9 Procedura testowania

1. W ramach tego zadania zostaną przeprowadzone wszystkie testy opisane w Umowie i Dokumentacji. Celem testów jest weryfikacja przez Zamawiających, czy wszystkie prace wykonane w trakcie realizacji PZ zostały wykonane prawidłowo i zgodnie z założeniami funkcjonalnymi i jakościowymi. Testy będą przeprowadzane przez Wykonawcę przy współudziale Zamawiających jak i wskazanych przez Zamawiającego osób i podmiotów zewnętrznych.
2. Pozytywne zakończenie testów wraz z usunięciem wskazanych Wad, dla poszczególnych Komponentów/Produktów oraz całego PZ, jest warunkiem niezbędnym aby dokonać odbiorów w ramach poszczególnych Etapów oraz Odbioru końcowego.
3. Procedura dotyczy Testów funkcjonalnych Komponentów poprzedzających Odbiór komponentu, zgodnie z Harmonogramem Wdrożenia.

---

#### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

4. Termin i czas przeprowadzenia poszczególnych testów funkcjonalnych zostanie określony w Harmonogramie Wdrożenia.

#### 4.10 Procedury odbiorowe

- 1) Do każdej dostawy będzie sporządzony protokół odbioru podpisany przez uprawnionych przedstawicieli stron. Protokół odbioru musi zawierać co najmniej: datę dostarczenia, dane identyfikacyjne, informację jakiego Komponenty dotyczy, numer pozycji umowy, której dotyczy przedmiot zamówienia oraz informację, że dostarczony przedmiot zamówienia jest zgodny ilościowo z wymaganiami niniejszej umowy. Przy dostawie i odbiorze przedmiotu zamówienia musi być obecny przedstawiciel Zamawiającego oraz uprawniony do tego przedstawiciel Wykonawcy.
- 2) Odbiór końcowy PZ ma na celu potwierdzenie wykonania wszystkich zadań wynikających z Umowy, w tym odebrania wszystkich Komponentów i Etapów oraz dostarczenia wymaganej zamówieniem Dokumentacji. Dokonanie Odbioru końcowego bez uwag zakończy realizację PZ.
- 3) Procedurę odbioru opisuje Załącznik 2.02 do SIWZ.

#### 4.11 Dokumentacja powykonawcza

- 1) Szczegółowy zakres dokumentacji powykonawczej został opisany w słowniku do niniejszego dokumentu (Załącznik nr 10 do SIWZ).
- 2) Dokumentacja Powykonawcza musi w szczególności zawierać numery seryjne dostarczonych urządzeń powiązane z ich fizyczną lokalizacją, listę adresów sprzętowych MAC interfejsów sieciowych (lista ta musi być dostarczona również w formie elektronicznej) oraz mapę połączeń. Wszystkie połączenia kablowe muszą być oznaczone z obu stron etykietami pozwalającymi na ich jednoznaczną identyfikację i zlokalizowanie na dostarczonej z Dokumentacją Powykonawczą mapie połączeń.
- 3) Wykonawca opíše szczegółowo informacje na temat zmian poczynionych w konfiguracji Istniejącego systemu informatycznego każdego PL.

#### 4.12 Instruktaże stanowiskowe

- 1) Wykonawca zaplanuje w uzgodnieniu z PL Instruktaże stanowiskowe w wymiarze nie mniejszym niż wskazany w pkt 2 dla wszystkich Zamawiających. Instruktaże stanowiskowe zostaną przeprowadzone w miejscach instalacji lub innych uzgodnionych z Zamawiającym np. dedykowane

- sale (w takim przypadku sprzęt dla pokazu zapewnia Wykonawca), dla całej Infrastruktury sprzętowej oraz Oprogramowania z zakresu obsługi, administracji i utrzymania.
- 2) Wykonawca ustali z poszczególnymi Zamawiającymi harmonogram przeprowadzania instruktarzy stanowiskowych na etapie tworzenia DPR. Harmonogram ten może ulec zmianie na etapie realizacji za wyraźną zgodą Zamawiającego na pisemną prośbę Wykonawcy. Wykonawca odpowiada za realizację minimalnych ilości godzin instruktażu w terminach realizacji Umowy.
  - 3) Wymiar Instruktaży stanowiskowych nie może być mniejszy niż (w godzinach dla każdej Placówki):
    - a) Dla PL07, PL08, PL12.1, PL18, PL19
      - i) Przełączniki dostępowe (rozdziały 8.3 – 8.7) – 50 godzin
      - ii) Przełączniki centralne (8.8 -8.9) – 30 godzin
      - iii) Urządzenia sieci bezprzewodowej (rozdziały 8.13-8.17) – 40 godzin
      - iv) Firewall – 60 godzin (z wyłączeniem PL07)
      - v) Oprogramowanie Zarządzające – 60 godzin
    - b) Dla PL01, PL05, PL14, PL16:
      - i) Przełączniki dostępowe (rozdziały 8.3 – 8.7) – 25 godzin
      - ii) Przełączniki centralne (8.8 -8.9) – 16 godzin
      - iii) Urządzenia sieci bezprzewodowej (rozdziały 8.13-8.17) – 20 godzin
      - iv) Firewall – 30 godzin
      - v) Oprogramowanie Zarządzające – 40 godzin
    - c) Dla PL02, PL06, PL10, PL11, PL17
      - i) Przełączniki dostępowe (rozdziały 8.3 – 8.7) – 16 godzin
      - ii) Przełączniki centralne (8.9 -8.9) – 10 godzin
      - iii) Urządzenia sieci bezprzewodowej (rozdziały 8.13-8.17) – 20 godzin
      - iv) Firewall – 16 godzin
      - v) Oprogramowanie Zarządzające – 25 godzin (z wyłączeniem PL02 i PL06)

Dopuszcza się przeniesienie godzin pomiędzy poszczególnymi rodzajami urządzeń na pisemną prośbę Zamawiającego w ramach przysługujących danemu podmiotowi godzin.

  - 4) PL każdorazowo po wykorzystaniu części puli godzin Instruktaży stanowiskowych zwróci się do Wykonawcy ze zleceniem odpowiednich prac łącznie z wymiarem godzinowym przeznaczonym na zadanie.
  - 5) Tematyka instruktażu stanowiskowego musi obejmować wszelkie czynności niezbędne do poprawnej eksploatacji dostarczonego systemu, w tym modyfikacje topologii połączeń i architektury, wymiany komponentów sprzętowych oraz obsługę interfejsów zarządzających (zarówno poprzez konsolę graficzną jak i tekstową). Instruktaże stanowiskowe będą prowadzone natywnie w języku polskim i obejmą w szczególności:
    - a) Zapoznanie i wdrożenie zasad funkcjonowania architektury i układu topologii sieci
    - b) Budowę i konfigurację wszystkich rodzajów dostarczanych urządzeń
    - c) Pomoc użytkownikom w korzystaniu z oprogramowania,

- d) Pomoc w administracji i zarządzaniu,
  - e) Kreowanie i utrzymanie polityki konfiguracji zabezpieczeń i backupu sieci
  - f) Procedury postępowania w przypadku incydentów
  - g) konsultacje.
- 6) Wykonawca wykona i uzgodni z Zamawiającymi plan instruktaży stanowiskowych w etapie wykonania Dokumentacji Projektowej.
- 7) Administratorzy techniczni po zakończeniu instruktaży muszą w szczególności umieć wykonywać czynności administracji, a także instalacji oprogramowania, znać i umieć realizować procedury backupu, znać wytyczne w zakresie polityki bezpieczeństwa i umieć je stosować. Ponadto powinni znać typowe zagrożenia i problemy związane z funkcjonowaniem sieci, a także sposoby ich przeciwdziałaniu, wykrywaniu i usuwaniu. Powinni umieć instalować, konfigurować, rekonfigurować, monitorować i prawidłowo eksploatować dostarczony sprzęt i oprogramowanie, jak również znać jego wdrożoną konfigurację.
- 8) W przypadku potrzeby Zamawiający zapewniają we własnym zakresie pomieszczenia dla przeprowadzenia Instruktaży stanowiskowych. Wykonawca może realizować Instruktaże stanowiskowe również na stanowiskach pracy pracowników PL.
- 9) Instruktaże muszą zostać przeprowadzone przez certyfikowanych inżynierów bądź trenerów z prowadzonego przez nich zakresu.

#### 4.13 Szkolenia specjalistyczne

- 1) Wykonawca zaplanuje w uzgodnieniu z Podmiotem Leczniczym szkolenia specjalistyczne dla Zamawiającego w wymiarze:
- a) Dla PL12.1,

Rodzaj szkolenia	Minimalna liczba dni w szkoleniu	liczba osób na szkolenie
Konfiguracja, administracja przełączników dostępowych	3	6
Konfiguracja, administracja przełączników centralnych	2	6
Konfiguracja, administracja Firewall	5	6



Konfiguracja, administracja rozwiązania sieci bezprzewodowej	3	6
Konfiguracja, administracja Oprogramowania Zarządzającego	3	6
Bezpieczeństwo sieci	3	6

b) Dla PL07, PL19

Rodzaj szkolenia	Minimalna liczba dni w szkoleniu	liczba osób na szkolenie
Konfiguracja, administracja przełączników dostępowych	3	4
Konfiguracja, administracja przełączników centralnych	2	4
Konfiguracja, administracja Firewall	5	4 (z wyłączeniem PL07 z powodu braku dostawy Firewall)
Konfiguracja, administracja rozwiązania sieci bezprzewodowej	3	4
Konfiguracja, administracja Oprogramowania Zarządzającego	3	4
Bezpieczeństwo sieci	3	4

c) PL18

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

Rodzaj szkolenia	Minimalna liczba dni w szkoleniu	liczba osób na szkolenie
Konfiguracja, administracja przełączników dostępowych	3	3
Konfiguracja, administracja przełączników centralnych	2	3
Konfiguracja, administracja Firewall	5	3
Konfiguracja, administracja rozwiązania sieci bezprzewodowej	3	3
Konfiguracja, administracja Oprogramowania Zarządzającego	3	3
Bezpieczeństwo sieci	3	3

d) PL05, PL16:

Rodzaj szkolenia	Minimalna liczba dni w szkoleniu	liczba osób na szkolenie
Konfiguracja, administracja przełączników dostępowych	3	2
Konfiguracja, administracja przełączników centralnych	2	2
Konfiguracja, administracja Firewall	5	2

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

Konfiguracja, administracja rozwiązania sieci bezprzewodowej	3	2
Konfiguracja, administracja Oprogramowania Zarządzającego	3	2
Bezpieczeństwo sieci	3	2

e) Dla PL01, PL02, PL08, PL06, PL10 ,PL11, PL14, PL17

Rodzaj szkolenia	Minimalna liczba dni w szkoleniu	liczba osób na szkolenie
Konfiguracja, administracja przełączników dostępowych	3	1
Konfiguracja, administracja przełączników centralnych	2	1
Konfiguracja, administracja Firewall	5	1
Konfiguracja, administracja rozwiązania sieci bezprzewodowej	3	1
Konfiguracja, administracja Oprogramowania Zarządzającego	3	1 (z wyłączeniem PL02 i PL06 z powodu braku dostawy Oprogramowania Zarządzającego)
Bezpieczeństwo sieci	3	1

2) Poniżej przedstawiono minimalny przykładowy zakres dla poszczególnych szkoleń. Dopuszcza się wymiennieść poszczególnych zakresów jeśli pozostają spójne w swoim zakresie oraz tematyce.

1. Konfiguracja, administracja przełączników dostępowych

Celem szkolenia jest poznanie budowy, funkcjonalności oraz umiejętności administracji przełącznikami dostępowymi dostarczanymi w ramach postępowania.

Minimalny zakres szkolenia:

- a) Omówienie rozwiązania przełączników dostępowych dostarczanego w ramach postępowania w tym funkcjonalności punktów dostępowych oraz kontrolerów
- b) Omówienie podstawowych technologii zarządzania przełącznikami dostępowymi w tym konfiguracji portów, VLAN itp.
- c) Omówienie metod zarządzanie uwierzytelnieniem użytkowników
- d) Omówienie funkcjonalności oraz metod bieżącej administracji dostarczanego rozwiązania
- e) Omówienie możliwości redundancji i konfiguracji nadmiarowej
- f) Omówienie konfiguracja bezpieczeństwa dostępu do sieci LAN za pomocą dostępnych w rozwiązaniu rozwiązań
- g) Omówienie funkcji monitorowania sieci i sposób rozwiązywania problemów

Za edycję szkolenia " Konfiguracja, administracja przełączników dostępowych " lub równoważnego uznaje się:

- a) Szkolenie " Konfiguracja, administracja przełączników dostępowych" trwające nie mniej niż 3 dni szkoleniowe.
- b) Szkolenie prowadzone w języku polskim, w formie stacjonarnej, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę. Wykonawca winien zapewnić nocleg uczestnikom oraz pełne wyżywienie (min. Śniadanie i obiad).
- c) Przeprowadzenie egzaminu certyfikującego z wiedzy autoryzowanego przez producenta rozwiązania przeprowadzanego przez autoryzowane centrum certyfikacyjne. Pozytywny wynik egzaminu skutkuje wydaniem certyfikatu potwierdzającego jego realizację. Nie dopuszcza się wydania Vouchera na egzamin. Wykonawca jest zobowiązany uzgodnić z Zamawiającym termin realizacji egzaminu jeśli odbywa się on w innym terminie niżeli szkolenie. Dzień egzaminu nie jest liczony jako dzień szkoleniowy.
- d) Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
- e) Grupa szkoleniowa może liczyć maksymalnie 15 osób. Każdy uczestnik musi posiadać własne stanowisko szkoleniowe.
- f) Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, z równomiernym rozłożeniem ich realizacji, z uwzględnieniem zastrzeżenia, że Zamawiający

może nie mieć możliwości skierowania wszystkich osób zgłoszonych na dany temat w jednym terminie.

- g) Uczestnicy powinni otrzymać materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli materiały w języku polskim są niedostępne.

## 2. Konfiguracja, administracja przełączników centralnych

Celem szkolenia jest poznanie budowy, funkcjonalności oraz umiejętności administracji przełącznikami centralnymi dostarczonymi w ramach postępowania.

Minimalny zakres szkolenia:

- a) Omówienie rozwiązania przełączników centralnych dostarczanego w ramach postępowania w tym funkcjonalności punktów dostępowych oraz kontrolerów
- b) Omówienie podstawowych technologii zarządzania przełącznikami centralnymi
- c) Omówienie funkcjonalności oraz metoda bieżącej administracji dostarczanego rozwiązania
- d) Omówienie metod zarządzanie uwierzytelnieniem użytkowników
- e) Omówienie możliwości redundancji i konfiguracji nadmiarowej
- f) Omówienie konfiguracja bezpieczeństwa dostępu do sieci LAN za pomocą dostępnych w rozwiązaniu rozwiązań
- g) Omówienie funkcji monitorowania sieci i sposób rozwiązywania problemów

Za edycję szkolenia " Konfiguracja, administracja przełączników centralnych" lub równoważnego uznaje się:

- a) Szkolenie " Konfiguracja, administracja przełączników centralnych" trwające nie mniej niż 3 dni szkoleniowe.
- b) Szkolenie prowadzone w języku polskim, w formie stacjonarnej, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę. Wykonawca winien zapewnić nocleg uczestnikom oraz pełne wyżywienie (min. Śniadanie i obiad).
- c) Przeprowadzenie egzaminu certyfikującego z wiedzy autoryzowanego przez producenta rozwiązania przeprowadzanego przez autoryzowane centrum certyfikacyjne. Pozytywny wynik egzaminu skutkuje wydaniem certyfikatu potwierdzającego jego realizację. Nie dopuszcza się wydania Vouchera na egzamin. Wykonawca jest zobowiązany uzgodnić z Zamawiającym termin realizacji egzaminu jeśli odbywa się on w innym terminie niżeli szkolenie. Dzień egzaminu nie jest liczony jako dzień szkoleniowy.
- d) Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
- e) Grupa szkoleniowa może liczyć maksymalnie 15 osób. Każdy uczestnik musi posiadać własne stanowisko szkoleniowe.

- f) Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, z równomiernym rozłożeniem ich realizacji, z uwzględnieniem zastrzeżenia, że Zamawiający może nie mieć możliwości skierowania wszystkich osób zgłoszonych na dany temat w jednym terminie.
- g) Uczestnicy powinni otrzymać materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli materiały w języku polskim są niedostępne.

### 3. Konfiguracja, administracja Firewall

Celem szkolenia jest poznanie budowy, funkcjonalności oraz umiejętności administracji Firewallami dostarczonymi w ramach postępowania.

Minimalny zakres szkolenia:

- a) Omówienie rozwiązania Firewall w ramach postępowania w tym funkcjonalności punktów dostępowych oraz kontrolerów
- b) Omówienie podstawowych technologii zarządzania przełącznikami dostępowymi w tym konfiguracji portów, VLAN itp.
- c) Omówienie funkcjonalności oraz metod bieżącej administracji dostarczanego rozwiązania
- d) Omówienie metod zarządzanie uwierzytelnieniem użytkowników
- e) Omówienie możliwości redundancji i konfiguracji nadmiarowej
- f) Omówienie konfiguracja bezpieczeństwa dostępu do sieci LAN za pomocą dostępnych w rozwiązaniu rozwiązań
- g) Omówienie funkcji monitorowania sieci i sposób rozwiązywania problemów

Za edycję szkolenia "Konfiguracja, administracja Firewall" lub równoważnego uznaje się:

- a) Szkolenie " Konfiguracja, administracja Firewall" trwające nie mniej niż 5 dni szkoleniowych.
- b) Szkolenie prowadzone w języku polskim, w formie stacjonarnej, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę. Wykonawca winien zapewnić nocleg uczestnikom oraz pełne wyżywienie (min. Śniadanie i obiad).
- c) Przeprowadzenie egzaminu certyfikującego z wiedzy autoryzowanego przez producenta rozwiązania przeprowadzanego przez autoryzowane centrum certyfikacyjne. Pozytywny wynik egzaminu skutkuje wydaniem certyfikatu potwierdzającego jego realizację. Nie dopuszcza się wydania Vouchera na egzamin. Wykonawca jest zobowiązany uzgodnić z Zamawiającym termin realizacji egzaminu jeśli odbywa się on w innym terminie niżeli szkolenie. Dzień egzaminu nie jest liczony jako dzień szkoleniowy.
- d) Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
- e) Grupa szkoleniowa może liczyć maksymalnie 15 osób. Każdy uczestnik musi posiadać własne stanowisko szkoleniowe.

- f) Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, z równomiernym rozłożeniem ich realizacji, z uwzględnieniem zastrzeżenia, że Zamawiający może nie mieć możliwości skierowania wszystkich osób zgłoszonych na dany temat w jednym terminie.
- g) Uczestnicy powinni otrzymać materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli materiały w języku polskim są niedostępne.

#### 4. Konfiguracja, administracja rozwiązania sieci bezprzewodowej

Celem szkolenia jest poznanie budowy, funkcjonalności oraz umiejętności administracji rozwiązaniem sieci bezprzewodowej dostarczanego w ramach postępowania.

Minimalny zakres szkolenia:

- a) Omówienie rozwiązania sieci bezprzewodowej dostarczanego w ramach postępowania w tym funkcjonalności punktów dostępowych oraz kontrolerów
- b) Omówienie podstawowych technologii WLAN, koncepcji standardu 802.11
- c) Omówienie funkcjonalności oraz metod bieżącej administracji dostarczanego rozwiązania
- d) Omówienie możliwości zarządzania uwierzytelnieniem użytkowników
- e) Omówienie możliwości redundancji i konfiguracji nadmiarowej
- f) Omówienie konfiguracji bezpieczeństwa dostępu do sieci WLAN za pomocą dostępnych w rozwiązaniu rozwiązań (np. reguł, ról, grup itp.)
- g) Omówienie pasma częstotliwości radiowych i kanałów oraz standardów stosowanych do ich realizacji
- h) Omówienie koncepcji pokrycia częstotliwości radiowych i zakłóceń
- i) Omówienie funkcji monitorowania sieci i sposób rozwiązywania problemów

Za edycję szkolenia "Konfiguracja, administracja przełączników dostępowych" lub równoważnego uznaje się:

- a) Szkolenie " Konfiguracja, administracja przełączników dostępowych" trwające nie mniej niż 3 dni szkoleniowe.
- b) Szkolenie prowadzone w języku polskim, w formie stacjonarnej, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę. Wykonawca winien zapewnić nocleg uczestnikom oraz pełne wyżywienie (min. Śniadanie i obiad).
- c) Przeprowadzenie egzaminu certyfikującego z wiedzy autoryzowanego przez producenta rozwiązania przeprowadzanego przez autoryzowane centrum certyfikacyjne. Pozytywny wynik egzaminu skutkuje wydaniem certyfikatu potwierdzającego jego realizację. Nie dopuszcza się wydania Vouchera na egzamin. Wykonawca jest zobowiązany uzgodnić z Zamawiającym

termin realizacji egzaminu jeśli odbywa się on w innym terminie niżeli szkolenie. Dzień egzaminu nie jest liczony jako dzień szkoleniowy.

- d) Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
- e) Grupa szkoleniowa może liczyć maksymalnie 15 osób. Każdy uczestnik musi posiadać własne stanowisko szkoleniowe.
- f) Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, z równomiernym rozłożeniem ich realizacji, z uwzględnieniem zastrzeżenia, że Zamawiający może nie mieć możliwości skierowania wszystkich osób zgłoszonych na dany temat w jednym terminie.
- g) Uczestnicy powinni otrzymać materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli materiały w języku polskim są niedostępne.

#### 5. Konfiguracja, administracja Oprogramowania Zarządzającego

Celem szkolenia jest poznanie budowy, funkcjonalności oraz umiejętności administracji Firewallami dostarczonymi w ramach postępowania.

Minimalny zakres szkolenia:

- a) Omówienie rozwiązania Oprogramowania Zarządzającego w ramach postępowania w tym funkcjonalności punktów dostępowych oraz kontrolerów
- b) Omówienie podstawowych technologii Oprogramowania Zarządzającego
- c) Omówienie funkcjonalności oraz metod bieżącej administracji dostarczanego rozwiązania
- d) Omówienie metod zarządzanie uwierzytelnieniem użytkowników
- e) Omówienie możliwości redundancji i konfiguracji nadmiarowej
- f) Omówienie konfiguracja bezpieczeństwa dostępu do sieci LAN za pomocą dostępnych w rozwiązaniu rozwiązań
- g) Omówienie funkcji monitorowania sieci i sposób rozwiązywania problemów

Za edycję szkolenia "Konfiguracja, administracja Oprogramowania Zarządzającego" lub równoważnego uznaje się:

- a) Szkolenie " Konfiguracja, administracja Oprogramowania Zarządzającego" trwające nie mniej niż 3 dni szkoleniowe.
- b) Szkolenie prowadzone w języku polskim, w formie stacjonarnej, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę. Wykonawca winien zapewnić nocleg uczestnikom oraz pełne wyżywienie (min. Śniadanie i obiad).
- c) Przeprowadzenie egzaminu certyfikującego z wiedzy autoryzowanego przez producenta rozwiązania przeprowadzanego przez autoryzowane centrum certyfikacyjne. Pozytywny wynik egzaminu skutkuje wydaniem certyfikatu potwierdzającego jego realizację. Nie dopuszcza się



wydania Vouchera na egzamin. Wykonawca jest zobowiązany uzgodnić z Zamawiającym termin realizacji egzaminu jeśli odbywa się on w innym terminie niżeli szkolenie. Dzień egzaminu nie jest liczony jako dzień szkoleniowy.

- d) Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
- e) Grupa szkoleniowa może liczyć maksymalnie 15 osób. Każdy uczestnik musi posiadać własne stanowisko szkoleniowe.
- f) Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, z równomiernym rozłożeniem ich realizacji, z uwzględnieniem zastrzeżenia, że Zamawiający może nie mieć możliwości skierowania wszystkich osób zgłoszonych na dany temat w jednym terminie.
- g) Uczestnicy powinni otrzymać materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli materiały w języku polskim są niedostępne.

#### 6. Bezpieczeństwo sieci / testy penetracyjne

Celem szkolenia jest poznanie metod ochrony sieci przed zagrożeniami.

Zakres szkolenia:

- a) Elementy bezpieczeństwa informacji
- b) Testy penetracyjne - jako metoda testowania bezpieczeństwa sieci
- c) Modyfikacja komunikacji sieciowej
- d) Bezpieczeństwo sieci – Ethernet
- e) Bezpieczeństwo warstwy 3 modelu OSI
- f) Firewall
- g) Bezpieczeństwo IPsec
- h) Bezpieczeństwo protokołów routingu
- i) Bezpieczeństwo web
- j) Systemy klasy IPS oraz firewall aplikacyjne
- k) Podatności klasy buffer overflow
- l) Realizacja przykładowego testu penetracyjnego w LAB

Za edycję szkolenia "Bezpieczeństwo sieci / testy penetracyjne" lub równoważnego uznaje się:

- a) Szkolenie " Bezpieczeństwo sieci / testy penetracyjne" trwające nie mniej niż 3 dni szkoleniowe.
- b) Szkolenie prowadzone w języku polskim, w formie stacjonarnej, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę. Wykonawca winien zapewnić nocleg uczestnikom oraz pełne wyżywienie (min. Śniadanie i obiad).
- c) Przeprowadzenie testu sprawdzającego poziom nabytej na szkoleniu wiedzy Test przeprowadzony w języku polskim w ostatnim dniu szkolenia.

---

#### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

- d) Za dzień szkoleniowy przyjmuje się min. 8 godzin lekcyjnych (45 min).
  - e) Grupa szkoleniowa może liczyć maksymalnie 15 osób. Każdy uczestnik musi posiadać własne stanowisko szkoleniowe.
  - f) Szkolenia powinny być przeprowadzone w terminach uzgodnionych z Zamawiającym, z równomiernym rozłożeniem ich realizacji, z uwzględnieniem zastrzeżenia, że Zamawiający może nie mieć możliwości skierowania wszystkich osób zgłoszonych na dany temat w jednym terminie.
  - g) Uczestnicy powinni otrzymać materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli materiały w języku polskim są niedostępne.
  - h) Uczestnicy powinni otrzymać zaświadczenie bądź certyfikat po ukończeniu szkolenia.
- 2) Za równoważne, Zamawiający uzna szkolenia obejmujące co najmniej przedmiot zawarty w szkoleniach o wyżej wymienionych nazwach – taka sama tematyka przedmiotowych szkoleń, taki sam czas wymagany do ich przeprowadzenia, taki sam zakres materiałów szkoleniowych dla uczestników szkoleń.
  - 3) Poszczególne szkolenia (z wyjątkiem szkolenia Bezpieczeństwo sieci / testy penetracyjne) muszą dotyczyć Infrastruktury sprzętowej dostarczanej w ramach postępowania oraz być szkoleniami autoryzowanymi przez producenta.
  - 4) Wykonawca odpowiada za ustalenie terminu z poszczególnymi uczestnikami (potwierzonego u koordynatora projektu w poszczególnych Placówkach), rezerwacje zakwaterowania oraz organizacji wyżywienia.
  - 5) Wszystkie szkolenia oraz egzaminy muszą zostać zrealizowane do dnia podpisania Protokołu Odbioru Końcowego.
  - 6) Wykonawca nie jest zobligowany do opłacenia lub zorganizowania egzaminu powtórkowego w przypadku niezaliczenia egzaminu przez użytkownika.

#### 4.14 Inne zobowiązania Wykonawcy

- 1. Wykonawca ponosi wszelką i wyłączną odpowiedzialność za awarie wynikające z procesu rozbudowy i migracji w tym własnych działań, tak więc zaprojektowanie Infrastruktury sieciowej i wdrożenie musi uwzględniać potencjalne ryzyka, które mogą zaistnieć w trakcie czynności objętych zamówieniem.
- 2. Zakres prac Wykonawcy w trakcie fazy wdrożenia obejmuje przekazanie Zamawiającemu wszystkich haseł dostępowych i administracyjnych w formie papierowej oraz elektronicznej na trwałym nośniku danych (np. pamięć flash, płyta DVD) oraz udzielanie przez okres 4 tygodni po Odbiorze Końcowym wsparcia w rozwiązywaniu problemów powstających podczas wykonywania czynności administracyjnych w trybie 8x5 ( w godzinach 8-16 w dni robocze).

## 5. Opis specyficznych wymagań dla poszczególnych Podmiotów Leczniczych

### 5.1 PL01 - Wojewódzki Szpital Psychiatryczny im. prof. Tadeusza Bilikiewicza w Gdańsku

#### 5.1.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

#### 5.1.2 Wymagania konfiguracyjne.

Zamawiający ma prawo do odstąpienia od poniższych wymogów, ich zmiany lub zaproponowania nowych w uzgodnieniu z Wykonawcą na etapie opracowania DPR jeśli będzie to leżało w najlepszym interesie Zamawiającego.

CECHA	OPIS WYMAGAŃ
Opis	Kompleks składa się z 7 budynków. W chwili obecnej sieć LAN szpitala obejmuje 1 serwerownię (Główna w bud. 17) oraz <b>13</b> nowych punktów dystrybucyjnych PPD.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	W zakresie modernizacji sieci pasywnej wykonano nowe połączenia światłowodowe SM (12J) pomiędzy nową serwerownią a poszczególnymi budynkami w kompleksie do wszystkich nowych PPD Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ
Łącza Internetowe	PL posiada jedno łącza zewnętrzne i jest podłączony do Internetu
Specyficzne wymagania	W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania.

WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

## 5.2 PL02- Stacja Pogotowia Ratunkowego w Gdańsku

### 5.2.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.2.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Kompleks składa się z 2 głównych budynków. Przełączniki oraz Access Pointy będą instalowane w budynku głównym oraz budynku portierni.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	W zakresie modernizacji sieci pasywnej wykonano nowe połączenia światłowodowe SM pomiędzy nową serwerownią a budynkiem portierni(PPD) Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ
Łącza Internetowe	PL posiada jedno łącza zewnętrzne i jest podłączony do Internetu
Specyficzne wymagania	W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania.

## 5.3 PL05 - Pomorskie Centrum Reumatologiczne im. dr Jadwigi Titz-Kosko w Sopocie Sp. z o.o.

### 5.3.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.3.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
<b>Opis</b>	PL składa się z dwóch lokalizacji: Sopot, ul. Grunwaldzka 1-3 - 4 budynki Sopot, ul. 23-Marca 93. – 2 budynki
<b>Sieć LAN</b>	Zgodnie z opisem z pkt. 4.5 Obie lokalizacje PL05: ul. Grunwaldzka 1-3 i ul. 23 Marca 93 podłączone są łączem wewnętrznym o przepustowości 1 Gbps.
<b>Sieć WLAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Technologia okablowania światłowodowego</b>	W zakresie modernizacji sieci pasywnej dla każdej lokalizacji wykonano nowe połączenia światłowodowe MM pomiędzy GPD, a poszczególnymi budynkami do wszystkich nowych PPD. Szczegółowe informację na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ
<b>Łącza Internetowe</b>	PL posiada jedno łącza zewnętrzne i jest podłączony do Internetu
<b>Specyficzne wymagania</b>	Z uwagi na zabytkowy charakter kompleksu należy przewidzieć konieczność uzgadniania sposób montażu AP z konserwatorem zabytków. Koszt uzgodnień leży po stronie Wykonawcy.
<b>WAŻNE</b>	<b>PL05 realizuje równolegle projekt Centrum Opieki Geriatrycznej w Sopocie (COG) co rodzi konieczność integracji z PeZ w części LAN pasywnej i aktywnej skutkując możliwością przenikania się terminów realizacji niektórych części PeZ i koordynacji:</b>

CECHA	OPIS WYMAGAŃ
	<ol style="list-style-type: none"><li>1. Sieć pasywna dla COG uwzględniona jest w projekcie budowy kompleksu COG i została zrealizowana przez Wykonawcę. Natomiast przetącniki dostępowe/dystrybucyjne dla COG zostaną zakupione w ramach Projektu PeZ w celu ułatwienia integracji na poziomie LAN aktywnych poprzez zakup tego samego typu urządzeń oraz ich jednoczesną instalację i konfigurację we wszystkich lokalizacjach PL05.</li><li>2. Sieć pasywna dla drugiego budynku przy ul. 23 Marca 93 (Oddział reumatologiczny dla dzieci) została wykonana w ramach Projektu PeZ</li><li>3. Dla COG w ramach sieci LAN aktywnej w Projekcie PeZ zakupionych będzie: 14 szt. AP, 2 szt. PoE 24/10G, 4szt. PoE 48/10G, 2szt. Core A</li></ol> <p>Należy przewidzieć dwa kontrolery WIFI. Kontroler Wifi – 1szt. Grunwaldzka, 1szt. 23marca . Kontrolery muszą się synchronizować na bieżąco, a role prime pełnić będzie kontroler na ulicy Grunwaldzkiej.</p>

## 5.4 PL06 Centrum Zdrowia Psychicznego w Słupsku

### 5.4.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.4.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Kompleks składa się z 1 budynku.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	W PL istnieje okablowanie światłowodowe w technologii MM. Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ. Dokumentacja ta zostanie udostępniona Wykonawcy po zakończeniu realizacji postępowania na część pasywną Projektu PeZ.
Łącza Internetowe	PL posiada jedno łącza zewnętrzne i jest podłączony do Internetu
Specyficzne wymagania	Brak
WAŻNE	1) Budynek objęty jest opieką konserwatora zabytków 2) Serwerownia znajdują się na 4 piętrze budynku, a PPD na parterze (poziom 0)

## 5.5 PL07 Wojewódzki Szpital Specjalistyczny im. Janusza Korczaka w Słupsku Sp. z o.o.

### 5.5.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.5.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
<b>Opis</b>	PL składa się z dwóch lokalizacji: <ul style="list-style-type: none"> <li>• Słupsk, ul. Hubalczyków 1 - 2 budynki</li> <li>• Szpital w Ustce, Mickiewicza 12 – 1 budynek</li> </ul>
<b>Sieć LAN</b>	<ul style="list-style-type: none"> <li>• Zgodnie z opisem z pkt. 4.5</li> <li>• łączność pomiędzy lokalizacjami realizowana jest obecnie poprzez VPN site-to-site poprzez sieć Internet.</li> </ul>
<b>Sieć WLAN</b>	Zgodnie z opisem z pkt. 4.5 Sieć WLAN będzie wdrażana i uruchomiona w lokalizacji Ustka.
<b>Technologia okablowania światłowodowego</b>	W PL istnieje okablowanie światłowodowe w technologii MM Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na cześć pasywną Projektu PeZ
<b>Łącza Internetowe</b>	PL posiada dwa łącza zewnętrzne i jest podłączony do Internetu
<b>Specyficzne wymagania</b>	W PL07 należy wdrożyć Oprogramowanie Zarządzające dla całej infrastruktury sieciowej dostarczanej w ramach PZ zgodnie z opisem w pkt. 0
<b>WAŻNE</b>	Brak



## 5.6 PL08 Szpital dla Nerwowo i Psychiczenie Chorych im. St. Kryzana w Starogardzie Gdańskim

### 5.6.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.6.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Placówka posiada jedna lokalizację składającą się z 28 budynków.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii SM. W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe SM pomiędzy PPD i GPD. Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na cześć pasywną Projektu PeZ.
Łącza Internetowe	PL posiada jedno łącza zewnętrzne i jest podłączony do Internetu
Specyficzne wymagania	W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych.

## 5.7 PL10 Wojewódzki Ośrodek Terapii Uzależnień w Gdańsku

### 5.7.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiciu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.7.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
<b>Opis</b>	PL10 składa się z trzech lokalizacji: <ul style="list-style-type: none"> <li>• Gdańsk, Zakopiańska 37 – 1 budynek</li> <li>• Smażno 9 -1 budynek</li> <li>• Srebrniki 9 – nie bierze udziału w projekcie</li> </ul>
<b>Sieć LAN</b>	<ul style="list-style-type: none"> <li>• Zgodnie z opisem z pkt. 4.5</li> <li>• Dla każdej lokalizacji przygotować niezależną sieć LAN</li> <li>• Wszystkie lokalizacje połączyć min. VPN L2L</li> </ul>
<b>Sieć WLAN</b>	<ul style="list-style-type: none"> <li>• Zgodnie z opisem z pkt. 4.5</li> <li>• W każdej lokalizacji będzie uruchomiona sieć WLAN</li> <li>• Zarządzanie AP w każdej lokalizacji centralnie przez główny kontroler</li> </ul> <p><b>Smażno:</b></p> <ul style="list-style-type: none"> <li>• Sieć WLAN należy skonfigurować z podsiecią dla pacjentów. W ramach dostępnych urządzeń sieciowych Zamawiający zapewni punkt styku obecnej sieci dla pacjentów z wdrażanym rozwiązaniem sieci WLAN.</li> </ul>
<b>Technologia okablowania światłowodowego</b>	PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii MM i SM. W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe MM i SM pomiędzy PPD i GPD. Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ. Dokumentacja ta zostanie udostępniona Wykonawcy po zakończeniu realizacji postępowania na część pasywną Projektu PeZ.
<b>Łącza Internetowe</b>	Każda lokalizacja PL10 posiada niezależne łącza Internetowe

CECHA	OPIS WYMAGAŃ
Specyficzne wymagania	Projektowana sieć LAN musi uwzględniać istniejącą sieć dla dzierżawionej usługi telefonii VoIP (W tym komunikację z siecią Internet do dostawcy)

## 5.8 PL11 Stacja Pogotowia Ratunkowego w Słupsku

### 5.8.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiciu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.8.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Placówka posiada jedną lokalizację na którą składa się 1 budynek.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	<ul style="list-style-type: none"> <li>Zgodnie z opisem z pkt. 4.5</li> <li>W lokalizacji będzie niezależnie zarządzana sieć bezprzewodowa.</li> </ul>
Technologia okablowania światłowodowego	<p>PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii MM.</p> <p>W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe MM pomiędzy PPD i GPD.</p> <p>Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ. Dokumentacja ta zostanie udostępniona Wykonawcy po zakończeniu realizacji postępowania na część pasywną Projektu PeZ.</p>
Łącza Internetowe	PL11 posiada łącza Internetowe niesymetryczne

## 5.9 PL12.1 COPERNICUS PL Sp. z o.o.

### 5.9.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.9.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	<p>PL12 składa się z pięciu głównych lokalizacji:</p> <ul style="list-style-type: none"> <li>• Gdańsk-Zaspa, Al. Jana Pawła II 50</li> <li>• Gdańsk, ul. Nowe Ogrody 1-6</li> <li>• Gdańsk, al. Zwycięstwa 31/32</li> <li>• Skłodowskiej-Curie 2, 80-210 Gdańsk</li> <li>• Powstańców Warszawskich 1-2, Gdańsk</li> </ul>
Sieć LAN	<p>Zgodnie z opisem z pkt. 4.5</p> <p>Zaspa:</p> <p>Dostarczane Przełączniki serwerowe zainstalowane w serwerowni podstawowej w której będzie umieszczona cała nowa infrastruktura serwerowo/macierzowa dostarczona w ramach PeZ</p>
Sieć WLAN	<ul style="list-style-type: none"> <li>• Zgodnie z opisem z pkt. 4.5</li> <li>• W każdej lokalizacji musi zostać wdrożona niezależnie zarządzana sieć bezprzewodowa.</li> <li>• W każdej z trzech lokalizacji muszą być dwa kontrolery obsługujące znajdujące się tam urządzenia AP.</li> </ul>
Technologia okablowania światłowodowego	<p>PL w każdej lokalizacji posiada pomiędzy PPD i GPD łącza światłowodowe w technologii MM/SM.</p> <p>W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe MM pomiędzy PPD i GPD.</p> <p>Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ</p>
Łącza Internetowe	Każda lokalizacja posiada niezależne, własne łącza Internetowe

CECHA	OPIS WYMAGAŃ
<p><b>Specyficzne wymagania</b></p>	<ul style="list-style-type: none"> <li>• W dokumentacji projektowej DPR dla tej PL należy zaprojektować łączność pomiędzy wszystkimi lokalizacjami w oparciu o architekturę ringu (jeśli to możliwe).</li> <li>• Dla Placówki dla każdego przełącznika Core (8.10) oraz każdego przełącznika serwerowego (8.11) należy dostarczyć moduły rozszerzeń rozbudowujące przełącznik o dodatkowe 8 portów SFP+ lub 8 portów MGig (1/2.5/5/10Gb/s) z interfejsem RJ-45 (jeśli dostarczony przełącznik posiada taką możliwość - nieobligatoryjne) lub 2 porty QSFP+. Wybór modułów dla poszczególnych przełączników nastąpi na etapie DPR. Dostarczane porty wyczerpują możliwość rozbudowy wymaganą w punkcie 8.10 i 8.11 tj. nie jest wymagana dodatkowa możliwość rozbudowy niniejszych przełączników.</li> <li>• W ramach PZ należy dostarczyć min. 6 modułów BiDi LC/LC 10Gbps SM (transmisja na jednej żyłce światłowodu).</li> </ul> <p><b>Zaspa:</b></p> <ul style="list-style-type: none"> <li>• Podczas tworzenia projektu dla PL 12- lokalizacja Zaspa należy uwzględnić iż w tej lokalizacji istnieje infrastruktura sieciowo/serwerowa zakupiona w ramach innego projektu i która musi pozostać bez zmian. W celu podłączenia obecnie posiadanych serwerów należy wykorzystać istniejące przełączniki CISCO 2960S (4 przełączniki) , które należy wyposażyć w moduły SPF (maksymalnie 4 przełączniki po 2 wkładki SFP) i wpiąć do przełączników Corowych w każdej z serwerowni doposażając wszystkie przełączniki (dostarczone w ramach PZ) w odpowiedniego typu moduły SPF. Ewentualnie obciążenia gwarancyjne istniejących przełączników nie przechodzą na Wykonawcę z tytułu rozbudowy ich o wkładki.</li> <li>• W ostatnich latach na swoim terenie realizował prace związane z remontami oddziałów Szpitalnych W ramach prac wykonano okablowanie strukturalne oraz dostarczono nowe przełączniki, m.in. urządzenia HP2960 z uplinkami światłowodowymi 1Gbps, bez możliwości budowania w stos. Z uwagi na fakt pełnej sprawności dostarczonych przełączników Zamawiający zamierza nadal eksploatować nieniejsze przełączniki W ramach niniejszego postępowania dostarczone zostaną przełączniki dystrybucyjne z modułami SPF/SPF+, dzięki którym będzie możliwe podpięcie każdego z</li> </ul>

CECHA	OPIS WYMAGAŃ
	eksploatowanych przełączników przy wykorzystaniu modułów 1Gbps i wolnych/budowanych (serwerownia zapasowa) włókien światłowodowych z przełącznikami Corowymi w każdej z serwerowni zapewniając tym samym możliwość zwiększenia przepustowości.

## 5.10 PL14 Szpital Dziecięcy Polanki im. Macieja Płazyńskiego w Gdańsku Sp. z o.o.

### 5.10.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.10.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Prosimy o zmianę na: Placówka posiada jedną główną lokalizację, na którą składa się 6 budynków (5 działalności operacyjnej i 1 - portiernia).
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii MM/SM. W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe MM pomiędzy PPD i GPD.  Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ
Łącza Internetowe	PL14 posiada łącza Internetowe niesymetryczne

## 5.11 PL16 Szpital Specjalistyczny w Prabutach Sp. z o.o.

### 5.11.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiciu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.11.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Placówka posiada jedną lokalizację na którą składa się 4 budynki.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii SM Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ
łącza MAN/WAN	brak
łącza Internetowe	PL posiada jedno łącza zewnętrzne do Internetu symetryczne 100 Mbps
Specyficzne wymagania	W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania.



## 5.12 PL17 Przemysłowy Zespół Opieki Zdrowotnej Sp. z o.o.

### 5.12.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiściu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.12.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
Opis	Placówka posiada jedną lokalizację na którą składa się 2 budynki.
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii MM. Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ. Dokumentacja ta zostanie udostępniona Wykonawcy po zakończeniu realizacji postępowania na część pasywną Projektu PeZ.
Łącza MAN/WAN	brak
Łącza Internetowe	PL posiada jedno łącza zewnętrzne do Internetu asymetryczne 10 Mbps
Specyficzne wymagania	W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania..

## 5.13 PL18 Szpital Specjalistyczny w Kościerzynie Sp. z o.o.

### 5.13.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.13.2 Wymagania konfiguracyjne.

CECHA	OPIS WYMAGAŃ
<b>Opis</b>	PL18 znajduje się w dwóch lokalizacjach: <ol style="list-style-type: none"><li>Kościerzyna, ul. Piechowskiego 36 – 3 budynki</li><li>Dzierżążno, ul. Szpitalna 36 – 11 budynków</li></ol>
<b>Sieć LAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Sieć WLAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Technologia okablowania światłowodowego</b>	W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe SM pomiędzy PPD i GPD. Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ
<b>Łącza MAN/WAN</b>	PL18 pomiędzy lokalizacjami posiada łącze dzierżawione 1 Gbps w warstwie 2
<b>Łącza Internetowe</b>	PL posiada dwa łącza zewnętrzne do Internetu symetryczne po 200 Mbps

CECHA	OPIS WYMAGAŃ
<b>Specyficzne wymagania</b>	<ol style="list-style-type: none"><li>1. W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych.</li><li>2. W ramach PZ należy dostarczyć min. 2 moduły BiDi LC/LC 1Gbps SM (transmisja na jednej żyłce światłowodu) kompatybilne z dostarczonymi przełącznikami core. Urządzenia te należy dobrać uwzględniając odległości pomiędzy dwoma lokalizacjami.</li><li>3. Przenieść i skonfigurować obecne połączenie pomiędzy lokalizacjami na dostarczane przełączniki w ramach Wdrożenia. Jeśli chodzi o lokalizację Kościerzyna łącze należy zakończyć w przełączniku core</li><li>4. Sieci WLAN w obu lokalizacja mają być zarządzane przez klaster kontrolerów WLAN umieszczony w lokalizacji Kościerzyno.</li><li>5. Na dostarczonych urządzeniach Firewall w lokalizacji Kościerzyno w ramach Wdrożenia skonfigurować mechanizmy redundancji i balansowania ruchem pomiędzy dwoma łączami Internetowymi.</li></ol>
<b>WAŻNE</b>	Uwzględnić dodatkowe urządzenie UTM dla tej lokalizacji, które umożliwiłoby zestawienia backupu VPN po sieci Internet z Kościerzyną. Dzierżno operacyjnie korzysta z systemów informatycznych/serwerów które znajdują się w Kościerzynie.

## 5.14 PL19.2 Szpitale Pomorskie Sp. z o.o.

### 5.14.1 Ilość i rodzaj urządzeń.

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 5.14.2 Wymagania konfiguracyjne.

PL 19.2.1 - Szpital Morski im PCK ul. Powstania Styczniowego Gdynia – 16 budynków

CECHA	OPIS WYMAGAŃ
Opis	<p>Placówka składa się z 3 lokalizacji:</p> <ul style="list-style-type: none"> <li>• Szpital Morski im PCK ul. Powstania Styczniowego 1 Gdynia – 16 budynków</li> <li>• Szpital so. Wincentego – Gdynia, ul Wójta Radtkego 1 – 3 budynki</li> <li>• Szpital Specjalistyczny im. F Ceynowy – Wejherowo ul. A Jagalskiego 10 – 6 budynków</li> </ul>
Sieć LAN	Zgodnie z opisem z pkt. 4.5
Sieć WLAN	Zgodnie z opisem z pkt. 4.5
Technologia okablowania światłowodowego	<p>W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe SM pomiędzy PPD i GPD.</p> <p>Szczegółowe informację na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ</p>
Łącza MAN/WAN	<p>PL posiada łącza dzierżawione do PL:</p> <ol style="list-style-type: none"> <li>1. Szpital Morski w Gdyni (pojedyncze/dwa czarne włókno/a)</li> <li>2. Szpital Zakaźny (2 włókna)</li> <li>3. Szpital w Wejherowie(2 włókna)</li> </ol> <p>Łącza zapasowe pomiędzy powyższymi lokalizacjami poprzez VPN typu Site-to-Site poprzez łącze Internetowe</p>
Łącza Internetowe	PL posiada dwa łącza zewnętrzne do Internetu symetryczne po 100 Mbps

CECHA	OPIS WYMAGAŃ
<b>Specyficzne wymagania</b>	<p>W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania.</p> <p>Dla Placówki dla każdego przełącznika Core (8.10) oraz każdego przełącznika serwerowego (8.11) należy dostarczyć moduły rozszerzeń rozbudowujące przełącznik o dodatkowe 2 porty QSFP+. Dostarczane porty wyczerpują możliwość rozbudowy wymaganą w punkcie 8.10 i 8.11 tj. nie jest wymagana dodatkowa możliwość rozbudowy niniejszych przełączników.</p>

PL 19.2. Szpital św. Wincentego - Gdynia, ul. Wójta Radtkego 1

CECHA	OPIS WYMAGAŃ
<b>Opis</b>	<p>Placówka składa się z 3 lokalizacji:</p> <ul style="list-style-type: none"> <li>• Szpital Morski im PCK ul. Powstania Styczniowego Gdynia – 16 budynków</li> <li>• Szpital św. Wincentego – Gdynia, ul Wójta Radtkego 1 – 3 budynki</li> </ul> <p>Szpital Specjalistyczny im. F Ceynowy – Wejherowo ul. A Jagalskiego 10 – 6 budynków</p>
<b>Sieć LAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Sieć WLAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Technologia okablowania światłowodowego</b>	<p>PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii SM.</p> <p>Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na część pasywną Projektu PeZ</p>
<b>Łącza MAN/WAN</b>	PL posiada (pojedyncze/dwa czarne włókno/a) do Szpitala Morskiego w Gdyni.
<b>Łącza Internetowe</b>	PL posiada jedno łącze zewnętrzne do Internetu symetryczne po 100 Mbps

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

CECHA	OPIS WYMAGAŃ
<b>Specyficzne wymagania</b>	<p>W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania..</p> <p>Dla Placówki dla każdego przełącznika Core (8.10) oraz każdego przełącznika serwerowego (8.11) należy dostarczyć moduły rozszerzeń rozbudowujące przełącznik o dodatkowe 2 porty QSFP+. Dostarczane porty wyczerpują możliwość rozbudowy wymaganą w punkcie 8.10 i 8.11 tj. nie jest wymagana dodatkowa możliwość rozbudowy niniejszych przełączników.</p>

PL 19.2.4 Szpital Specjalistyczny im. F. Ceynowy Sp. z o.o. -Wejcherowo, ul. dr. A. Jagalskiego 10

CECHA	OPIS WYMAGAŃ
<b>Opis</b>	<p>Placówka składa się z 3 lokalizacji:</p> <ul style="list-style-type: none"> <li>• Szpital Morski im PCK ul. Powstania Styczniowego Gdynia – 16 budynków</li> <li>• Szpital s.o. Wincentego – Gdynia, ul Wójta Radtkego 1 – 3 budynki</li> </ul> <p>Szpital Specjalistyczny im. F Ceynowy – Wejcherowo ul. A Jagalskiego 10 – 6 budynków</p>
<b>Sieć LAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Sieć WLAN</b>	Zgodnie z opisem z pkt. 4.5
<b>Technologia okablowania światłowodowego</b>	<p>PL posiada pomiędzy PPD i GPD łącza światłowodowe w technologii MM i SM.</p> <p>W zakresie modernizacji sieci pasywnej wykonano dodatkowe połączenia światłowodowe MM i SM pomiędzy PPD i GPD.</p> <p>Szczegółowe informacje na ten temat znajdują się w dokumentacji powykonawczej okablowania strukturalnego – postępowania na cześć pasywną Projektu PeZ</p>
<b>Łącza MAN/WAN</b>	PL posiada (pojedyncze/dwa czarne włókno/a) do Szpitala Morskiego w Gdyni.
<b>Łącza Internetowe</b>	PL posiada jedno łącza zewnętrzne do Internetu symetryczne po 100 Mbps

CECHA	OPIS WYMAGAŃ
<p><b>Specyficzne wymagania</b></p>	<p>W ramach realizacji PZ Wykonawca musi wdrożyć mechanizmy backupu konfiguracji urządzeń aktywnych dostarczanych w ramach postępowania..</p> <ol style="list-style-type: none"> <li>1. W dokumentacji projektowej DPR dla tej PL należy zaprojektować łączność pomiędzy wszystkimi ww. lokalizacjami (sieciami LAN Szpitali) w oparciu o architekturę gwiazdy (jeśli to możliwe).</li> <li>2. W ramach PZ należy dostarczyć odpowiednie min. 6 modułów BiDi LC/LC 10Gbps SM (transmisja na jednej żyłce światłowodu). Moduły należy dobrać dla dostarczanych urządzeń core, uwzględniając odległości pomiędzy Szpitalami.</li> <li>3. W ramach Wdrożenia należy skonfigurować połączenia pomiędzy lokalizacjami na dostarczonych urządzeniach core (jeśli to możliwe).</li> <li>4. Jako łącza backupowe pozostawić istniejące/skonfigurować dodatkowe połączenia z wykorzystaniem VPN (Site-to-Site) pomiędzy lokalizacjami.</li> <li>5. Na dostarczonym klastrze urządzeń Firewall w Szpitalu Morskim im. PCK Sp. z o.o. Gdynia w ramach Wdrożenia skonfigurować mechanizmy redundancji i balansowania ruchem pomiędzy dwoma łączami Internetowymi.</li> <li>6. Dla Placówki dla każdego przełącznika Core (8.10) oraz każdego przełącznika serwerowego (8.11) należy dostarczyć moduły rozszerzeń rozbudowujące przełącznik o dodatkowe 2 porty QSFP+. Dostarczane porty wyczerpują możliwość rozbudowy wymaganą w punkcie 8.10 i 8.11 tj. nie jest wymagana dodatkowa możliwość rozbudowy niniejszych przełączników.</li> </ol>

## 6. Specyfikacja ilościowa urządzeń aktywnych dla wszystkich PL

Zestawienie ilościowe urządzeń w rozbiu na poszczególne PL znajdują się w załączniku nr 1.01 do SIWZ Wzór Formularza Cenowego.

### 6.1 Sieć WLAN - urządzenia aktywne

LP.	NAZWA SKRÓCONA	RODZAJ URZĄDZENIA	ILOŚĆ (SZT)
1	AP	Access Point	1146
2	Kontroler WLAN Typ A	Kontroler sieci bezprzewodowej Typ A	8
3	Kontroler WLAN Typ B	Kontroler sieci bezprzewodowej Typ B	16
4	Kontroler WLAN Typ C	Kontroler sieci bezprzewodowej Typ C	8

### 6.2 Sieć przewodowa - urządzenia aktywne

LP.	NAZWA SKRÓCONA	RODZAJ URZĄDZENIA	ILOŚĆ (SZT)
1.	PoE 24/10G	Przełącznik Access LAN PoE 24/10G	189
2.	PoE 48/10G	Przełącznik Access LAN PoE 48/10G	10
3.	24G/10G	Przełącznik Access LAN 24G/10G	79
4.	48G/10G	Przełącznik Access LAN 48G/10G	418
5.	8G PoE	Przełącznik Access LAN 8G PoE	25
6.	Core	Przełącznik Core	59
7.	Serwerowy	Przełącznik serwerowy	32
8.	UTM Typ A	Firewall w HA i licencje UTM – Typ A	10
9.	UTM Typ B	Firewall w HA i licencje UTM – Typ B	8

#### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk  
tel. 58 32 68 524, faks 58 32 68 526  
e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE



LP.	NAZWA SKRÓCONA	RODZAJ URZĄDZENIA	ILOŚĆ (SZT)
10.	OZ	Oprogramowanie Zarządzające	12

## 7. Specyfikacja techniczna Oprogramowania Zarządzającego (OZ)

### 7.1 Podstawowe założenia dotyczące Oprogramowania Zarządzającego.

1. Do każdego PL należy dostarczyć lokalne oprogramowanie zarządzające z liczbą licencji wystarczającą do obsługi wszystkich dostarczanych w ramach postępowania przełączników, kontrolerów sieci bezprzewodowej i punktów dostępowych z danego PL oraz 20% zapas licencji na ilość urządzeń.
2. Wykonawca jest odpowiedzialny za zaprojektowanie, dostawy licencji i wdrożenie OZ ściśle dostosowanego jakościowo i ilościowo (urządzenia dostarczane w ramach niniejszego postępowania) do środowisk informatycznych Zamawiającego.
3. OZ wraz ze środowiskiem informatycznym (budowanym w ramach realizacji niniejszego postępowania) Zamawiającego będą tworzyć jednorodne, homogeniczne środowisko informatyczne umożliwiające w pełni na korzystanie z funkcjonalności Oprogramowania.
4. Oprogramowanie standardowe będzie zaprojektowane, dostarczone, skonfigurowane i wdrożone przez Wykonawcę zgodnie z niniejszym Opiszem przedmiotu zamówienia w szczególności w uzgodnieniu z Zamawiającymi.

W skład OZ wchodzić będzie sprzęt wraz z oprogramowaniem służący do monitorowania, realizacji reguł polityki dostępu, zarządzania logami oraz raportowania. OZ ma umożliwiać centralizację procesów zarządzania funkcjonalnościami urządzeń aktywnych dostarczonych w ramach PZ wraz z istniejącą infrastrukturą LAN PL.

OZ musi być realizować minimum poniższe funkcjonalności:

## 7.2 Wymagania techniczne Oprogramowania Zarządzającego.

CECHA	OPIS WYMAGAŃ
<b>Architektura</b>	<p>OZ musi być zbudowany w architekturze klient – serwer. OZ musi mieć budowę modułową, tak aby możliwe było doinstalowanie modułu dającego dodatkową funkcjonalność, która stanie się integralną częścią systemu, minimalnie::</p> <ul style="list-style-type: none"> <li>- Zarządzenia mechanizmami QoS w tym monitorowanie parametrów SLA</li> <li>- Audyt użytkowników z wykorzystaniem informacji z logów, przepływów sieciowych sFlow, NetStream v5 oraz analizy zawartości pakietów SMTP, FTP, http</li> <li>- Zarządzenie sieciami MPLS oraz sieciami VPN w oparciu o MPLS oraz VPLS</li> <li>- Zarządzanie dostępem zdalnym Ipsec/VPN</li> <li>- Zarządzanie urządzeniami typu Firewall</li> <li>- Wbudowany serwer TACACS</li> <li>- Obsługa informacji przesyłanych z wykorzystaniem sFlow oraz Netstream z urządzeń sieciowych oraz obrazowanie wyników</li> <li>- Funkcja monitorowania wydajności aplikacji</li> </ul>
<b>Wersja systemu</b>	OZ musi zostać dostarczony w najnowszej dostępnej na rynku wersji na dzień ostatecznego odbioru OZ-tu
<b>Redundancja</b>	System musi umożliwiać instalację rozproszoną na wielu maszynach (serwerach) fizycznych lub wirtualnych w celu uzyskania redundancji i wysokiej wydajności. System dostarczony musi być systemem redundantnym oraz mieć możliwość instalacji na minimum 2 maszynach fizycznych lub wirtualnych. Wykonawca musi dostarczyć wymagane oprogramowanie systemowe (licencję bazodanowe, systemy operacyjne itp.). Dostarczane licencję dodatkowe przechodzą na własność Zmawiającego.
<b>Licencja</b>	Do każdego PL należy dostarczyć lokalne oprogramowanie zarządzające z liczbą licencji wystarczającą do obsługi wszystkich dostarczanych w ramach postępowania przełączników, kontrolerów sieci bezprzewodowej i punktów dostępowych z danego PL oraz 20% zapas licencji na ilość urządzeń. Licencja nie może być ograniczona czasowo lub na ilość użytkowników mających dostęp do rozwiązania.
<b>Podstawowa funkcjonalność</b>	
1.	OZ musi posiadać funkcje umożliwiające automatyczne wykrywanie topologii sieci z użyciem protokołów SNMP, Telnet

### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

CECHA	OPIS WYMAGAŃ
2.	OZ musi posiadać funkcje monitorowania stanu urządzeń po protokole SNMP
3.	OZ musi posiadać funkcje konfiguracji urządzeń po protokole SNMP
4.	OZ musi umożliwiać zbieranie statystyk co najmniej z wykorzystaniem SNMP, RMON.
5.	Wsparcie monitoringu serwerów i innych urządzeń wspierających protokół SNMP
6.	OZ musi posiadać funkcje zarządzania konfiguracją urządzeń, tworzenia backupów oraz grupowego implementowania konfiguracji przechowywanych w OZ-cie na zarządzane urządzenia
7.	OZ musi posiadać funkcje archiwizacji konfiguracji i zarządzania obrazami oprogramowania urządzeń.
8.	OZ musi posiadać zcentralizowany mechanizm przeglądania zdarzeń w sieci, tzw. dashboard (skonsolidowany, syslog, trapy snmp i alarmy).
9.	OZ musi posiadać funkcje wysyłania alarmów np. e-mailem lub SMS'em
10.	OZ musi pozwalać na budowanie widoków przez administratora
11.	OZ musi posiadać funkcje generowania raportów w oparciu o szablony z możliwością dostosowywania ich do potrzeb klienta
12.	OZ musi posiadać narzędzia graficznej prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmian stanu tych urządzeń (stan portu, itp.) oraz występujących alarmów
13.	OZ musi posiadać wbudowane narzędzie do przeprowadzenia inwentaryzacji komponentów używanych w sieci w tym sprzętu i oprogramowania systemowego (firmware) urządzeń sieciowych
14.	OZ musi posiadać funkcje lokalizowania użytkowników po adresie IP lub MAC
15.	OZ musi posiadać wbudowane mechanizmy wspomagające wyszukiwanie, izolację problemów i ich rozwiązywanie
16.	OZ musi posiadać funkcje zdefiniowania polityki zmieniającej ustawienia sieci w przypadku wykrycia ataku sieciowego
17.	OZ musi posiadać funkcje tworzenia mapki sieciowej obrazującej połączenia sieciowe związane z zarejestrowanym atakiem sieciowym

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

CECHA	OPIS WYMAGAŃ
18.	OZ musi posiadać funkcje Telnet / SSH proxy umożliwiającą zarządzanie CLI przez przeglądarkę Internetową
19.	OZ musi posiadać funkcje zarządzania za pomocą urządzeń mobilnych tj. iPhone oraz urządzeniami z systemem Android
20.	OZ musi posiadać funkcje dostępu do sytemu zarządzania realizowaną przez przeglądarkę internetową (min. Chrome i Firefox)
21.	OZ musi posiadać funkcje podłączenia się i importu danych z serwera LDAP / Active Directory
22.	OZ musi posiadać funkcje zbierania informacji o konfiguracji urządzeń w sieci dzienników zdarzeń systemu, informacji o zasobach (np. mapy topologii sieci) i przesyłania tych informacji za pomocą FTP, SFTP, e-mail
23.	OZ musi posiadać funkcje tworzenia kont administratorskich z różnymi poziomami uprawnień oraz z możliwością przypisywania administratorów do grup urządzeń
24.	OZ musi posiadać funkcje zarządzania siecią wirtualną poprzez integracje SOAP z VMWare Virtual Center Server oraz Microsoft Hyper-V vManager.
25.	OZ musi mieć możliwość zarządzania siecią wirtualną dla serwerów Microsoft Hyper-V poprzez profil Power shell oraz WMI.
26.	OZ musi posiadać funkcje natywnie zaszyte funkcje zarządzania co najmniej dla 1000 modeli urządzeń.
27.	OZ musi posiadać funkcję automatycznej aktualizacji przez Internet.
28.	OZ musi posiadać funkcje implementacji rozproszonej na wielu serwerach
29.	OZ musi umożliwiać tworzenie kopii zapasowej na życzenie (on demand) i w regularnych odstępach czasowych (scheduled)
30.	OZ musi pozwalać na podział urządzeń w logiczne grupy reprezentujące oddziały, lokalizacje, budynki i inne definiowalne podgrupy
<b>Zarządzanie WLAN</b>	
1.	OZ musi zarządzać urządzeniami WLAN w zakresie: tworzenia list i zbierania informacji o kontrolerach WLAN, tworzenia list i zbierania informacji o punktach dostępowych WLAN

CECHA	OPIS WYMAGAŃ
2.	OZ musi podawać informacje o statusie urządzeń Wireless. Oprogramowanie musi zbierać i przedstawiać informacje kluczowe: <ol style="list-style-type: none"><li>1) Dla kontrolerów, co najmniej, status urządzenia</li><li>2) Dla punktów dostępowych, co najmniej: zbieranie i przedstawianie informacji o klientach WLAN, tworzenie statystyk z ilością podłączonych klientów oraz zajętością pasma urządzenia</li><li>3) Oprogramowania musi mieć możliwość przedstawienia logicznego i fizycznego obrazu sieci WLAN</li></ol>
3.	4) OZ musi pozwalać na wgranie planu budynku i rozmieszczenie na nim punktów dostępowych. Plany powinny być obsługiwane minimalnie w formatach: JPG, JPEG, PNG oraz CAD.
4.	5) Wykrywanie oraz tworzenie statystyk z prób połączeń obcych punktów dostępowych oraz klientów tzw. „Rogue AP”, „Rogue Client”.
5.	6) Możliwość tworzenia statystyk w oparciu o powiązanie klientów z SSID
6.	7) Tworzenie statystyk w oparciu o wykorzystanie i zajętość konkretnego kanału sieci bezprzewodowej

## 8. Specyfikacja techniczna urządzeń aktywnych

### 8.1 Wymagania ogólne

- 1) Wymagane w niniejszej specyfikacji parametry są parametrami minimalnymi.
- 2) Wszelkie nazwy własne użyte przy definiowaniu wymagań minimalnych stanowią punkt odniesienia dla standardów wymaganych przez Zamawiającego i nie stanowią warunku granicznego dla oferowanego sprzętu.
- 3) Zamawiający dopuszcza zastosowanie rozwiązań równoważnych w stosunku do cech podanych z użyciem nazw własnych.
- 4) Wszystkie dostarczone urządzenia muszą być wyposażone w komplet akcesoriów niezbędnych do uruchomienia i instalacji tak, aby po uruchomieniu osiągnęły wymaganą opisaną w PZ funkcjonalność.
- 5) Zamawiający wymaga, by dostarczone urządzenia były nowe i nieużywane wcześniej w żadnych projektach.
- 6) Wszystkie urządzenia muszą posiadać oznakowanie CE.
- 7) Wszystkie dostarczane urządzenia na dzień złożenia oferty nie mogą być w fazie end-of-life (EOL) lub nie może być wskazana data wejścia urządzenia w EOL (brak wsparcia producenta lub wycofanie urządzenia z oficjalnej dystrybucji).
- 8) Wszystkie urządzenia muszą współpracować z siecią energetyczną o parametrach: 230 V  $\pm$  10%, 50Hz (chyba, że w wymaganiach szczegółowych jest wyspecyfikowane inaczej).
- 9) Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w formie papierowej lub elektronicznej w języku polskim lub angielskim.
- 10) Wykonawca jest zobowiązany do doboru odpowiednich, do przewidywanych odległości pomiędzy poszczególnymi urządzeniami oraz istniejącym w projektowanym miejscu połączeniami, typów wkładek do interfejsów komunikacyjnych.
- 11) Dostarczane licencje (zarówno na funkcjonalności przełączników jak na oprogramowanie) muszą być permanentne tj. nie dopuszcza się ograniczeń czasowych w dostarczanych licencjach lub modelu subskrypcyjnym. Zamawiający dopuszcza subskrypcje czasowe na dostarczania aktualizacji baz np. dla niektórych funkcjonalności Firewall jednak w przypadku gdy bez aktualizacji funkcjonalność nadal jest dostępna.
- 12) Dla dostarczanych w ramach postępowania Infrastruktury oraz Oprogramowania wymagane jest objęciem co najmniej 5 letnią gwarancją producenta. Musi ona objąć obejmująca wszystkie elementy Infrastruktury (również zasilacze i wentylatory). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego

---

#### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

producenta. Dla infrastruktury której poprawne działanie wymienionych funkcjonalności wymagają dostarczenia subskrypcji wymaga się dostarczenia subskrypcji na co najmniej 5 lat.

13) W wypadku powzięcia wątpliwości, co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:

- a) zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z ofertą i OPZ (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację), oraz
- b) zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi, inspekcji produktów pod kątem ich zgodności z ofertą i OPZ oraz ważności i zakresu uprawnień licencyjnych.



## 8.2 Ogólne wymagania, wspólne dla wszystkich typów przełączników (punkty od 8.3 do 8.9)

- 1) Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
- 2) Funkcja autoryzacji użytkowników zgodna z 802.1x
- 3) Minimum 1GB pamięci RAM
- 4) Wsparcie dla funkcji Private VLAN lub równoważnego
- 5) Agregacja portów zgodna z 802.3ad LACP
- 6) Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
- 7) Obsługa IEEE 802.1s Multiple SpanningTree (MSTP) oraz IEEE 802.1w Rapid Spanning Tree Protocol (RSTP)
- 8) Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping
- 9) Wsparcie dla RADIUS Accounting
- 10) Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2 i 3, Telnet, SSH v.2, Web GUI (dostępne bezpośrednio na przełączniku), dedykowane oprogramowanie do zarządzania producenta przełącznika
- 11) Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI
- 12) Obsługa standardu 802.1p
- 13) Klasyfikacja ważności ruchu na bazie list kontroli dostępu, techniką IEEE 802.1p CoS, IP, DSCP lub Type of Service (ToS);
- 14) Funkcja mirroringu portów
- 15) Obsługa Syslog
- 16) Obsługa NTP lub SNTPv4
- 17) Obsługa protokołu Vlan Trunking Protocol (VTP) lub Multiple VLAN Registration Protocol (MVRP)
- 18) Obsługa ramek Jumbo
- 19) Obudowa dostosowana do montażu w szafie stelażowej 19". Wysokość 1U
- 20) Wszystkie funkcje muszą być dostępne bez licencji. Jeżeli do działania którejkolwiek z funkcji wymagana jest licencja to należy ją dostarczyć w ramach tego postępowania. Licencja nie może być ograniczona czasowo

### 8.3 Przełącznik Access LAN PoE 24/10G

CECHA	OPIS WYMAGAŃ
<b>Porty Ethernet</b>	Min. 24x 10/100/1000 PoE+, min budżet PoE 370W
<b>Porty dodatkowe</b>	Min. 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) - w tym dwa używane do łączenia w stos.
<b>Tablica MAC</b>	Min. 32000
<b>Obsługa VLAN</b>	Min. 4094 tagi VLAN oraz min. 2000 jednoczesnych sieci VLAN
<b>Stackowanie</b>	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 aktywnych urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klastery). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Do każdego przełącznika musi być dołożony kabel stackujący o długości co najmniej 1m.
<b>Szybkość przełączania</b>	Min. 128 Gbps
<b>Przepustowość</b>	Min. 95 Mpps
<b>Protokoły routingu</b>	statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów), RIPv2, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
<b>Wielkość tablicy routingu</b>	minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
<b>Zasilanie</b>	Napięcie zmienne: 230 V, 50 Hz. Maksymalny pobór mocy urządzenia (bez PoE) nie może przekraczać 120W Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
<b>Warunki środowiskowe</b>	Minimalny zakres temperatury pracy od 0°C do 45°C

## 8.4 Przełącznik Access LAN PoE 48/10G

CECHA	OPIS WYMAGAŃ
Porty Ethernet	Min. 48x 10/100/1000 PoE+ min. budżet PoE 370W
Porty dodatkowe	Min. 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) - w tym dwa używane do łączenia w stos.
Tablica MAC	Min. 32000
Obsługa VLAN	Min. 4094 tagi VLAN oraz min. 2000 jednoczesnych sieci VLAN
Stackowanie	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 aktywnych urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Do każdego przełącznika musi być dołożony kabel stackujący o długości co najmniej 1m.
Szybkość przełączania	Min. 176 Gbps
Przepustowość	Min. 112 Mpps
Protokoły routingu	statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów), RIPv6, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
Wielkość tablicy routingu	minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
Zasilanie	Napięcie zmienne: 230 V, 50 Hz. Maksymalny pobór mocy urządzenia (bez PoE) nie może przekraczać 180W Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
Warunki środowiskowe	Minimalny zakres temperatury pracy od 0°C do 45°C

## 8.5 Przełącznik Access LAN 24G/10G

CECHA	OPIS WYMAGAŃ
Porty Ethernet	Min. 24x 10/100/1000
Porty dodatkowe	Min. 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) - w tym dwa używane do łączenia w stos.
Tablica MAC	Min. 32000
Obsługa VLAN	Min. 4094 tagi VLAN oraz min. 2000 jednoczesnych sieci VLAN
Stackowanie	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 aktywnych urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Do każdego przełącznika musi być dołożony kabel stackujący o długości co najmniej 1m.
Szybkość przełączania	Min. 128 Gbps
Przepustowość	Min. 95 Mpps
Protokoły routingu	statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów), RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
Wielkość tablicy routingu	minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
Zasilanie	Napięcie zmienne: 230 V, 50 Hz. Maksymalny pobór mocy urządzenia nie może przekraczać 120W Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
Warunki środowiskowe	Minimalny zakres temperatury pracy od 0°C do 45°C

### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk  
tel. 58 32 68 524, faks 58 32 68 526  
e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

## 8.6 Przełącznik Access LAN 48G/10G

CECHA	OPIS WYMAGAŃ
Porty Ethernet	Min. 48x 10/100/1000
Porty dodatkowe	Min. 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) - w tym dwa używane do łączenia w stos.
Tablica MAC	Min. 32000
Obsługa VLAN	Min. 4094 tagi VLAN oraz min. 2000 jednoczesnych sieci VLAN
Stackowanie	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 aktywnych urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klastery). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Do każdego przełącznika musi być dołożony kabel stackujący o długości co najmniej 1m.
Szybkość przełączania	Min. 176 Gbps
Przepustowość	Min. 112 Mpps
Protokoły routingu	statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów), RIPv6, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
Wielkość tablicy routingu	minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
Zasilanie	Napięcie zmienne: 230 V, 50 Hz. Maksymalny pobór mocy urządzenia nie może przekraczać 120W Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
Warunki środowiskowe	Minimalny zakres temperatury pracy od 0°C do 45°C

## 8.7 Przełącznik Access LAN 8G PoE

CECHA	OPIS WYMAGAŃ
<b>Porty Ethernet</b>	Min. 8 x 10/100/1000 PoE+, min budżet mocy 125W
<b>Porty dodatkowe</b>	Min. 2 porty 10Gb SFP+, pozwalające na instalację wkładek SFP 1G oraz łączenie w stos
<b>Tablica MAC</b>	Min. 32000
<b>Obsługa VLAN</b>	Min. 4094 tagi VLAN oraz min. 2000 jednoczesnych sieci VLAN
<b>Stackowanie</b>	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 aktywnych urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Do każdego przełącznika musi być dołożony kabel stackujący o długości co najmniej 1m.
<b>Szybkość przełączania</b>	Min. 56 Gbps
<b>Przepustowość</b>	Min. 41 Mpps
<b>Protokoły routingu</b>	statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów), RIPv6, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów)
<b>Wielkość tablicy routingu</b>	minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6
<b>Zasilanie</b>	Napięcie zmienne: 230 V, 50 Hz. Maksymalny pobór mocy urządzenia nie może przekraczać 110W Wsparcie dla Energy-efficient Ethernet (EEE) IEEE 802.3az
<b>Warunki środowiskowe</b>	Minimalny zakres temperatury pracy od 0°C do 45°C Możliwość montażu w szafie RACK 19", wysokość 1U – jeżeli do montażu są wymagane dodatkowe akcesoria to należy je dostarczyć w ramach tego postępowania.

## 8.8 Przełącznik Core

CECHA	OPIS WYMAGAŃ
<b>Szybkość przełączania</b>	Minimum 480 Gb/s (nie licząc magistrali stackującej)
Przepustowość	Minimum 285 Mpps
<b>Interfejsy sieciowe 10Gb</b>	Przełącznik musi posiadać <b>minimum 16 portów 10G SFP+</b> . Nie dopuszcza się uzyskania portów SFP+ poprzez zastosowanie kabli rozszywających
<b>Interfejsy sieciowe 1Gb</b>	Przełącznik musi mieć możliwość obsługi portów o prędkości 1Gb Ethernet zależnie od wykorzystanej wkładki. Przełącznik musi mieć możliwość obsługi wkładki SFP w porcie SFP+
<b>Rozbudowa</b>	Możliwość rozbudowy o dodatkowe 8 portów SFP+ lub 2 porty QSFP+. Obydwie opcje muszą być dostępne w chwili składania oferty. Dodatkowe porty muszą być w pełni niezależne od portów podstawowych (rozbudowa nie jest wymagana w przypadku, gdy ilość portów w dostarczonym przełączniku jest odpowiednia większa niż wymagane minimum np. 24 porty SFP+ i 2 port QSFP+). Nie dopuszcza się uzyskania portów SFP+ poprzez zastosowanie kabli rozszywających
<b>Obsługa funkcjonalności STACK</b>	Przełącznik musi posiadać co najmniej 2 dedykowane porty umożliwiające łączenie w stos. Wydajność fizycznych portów stackujących co najmniej 40 Gbps na port. Oprogramowanie przełącznika musi umożliwiać połączenie co najmniej 10 aktywnych urządzeń w stos. Przełączniki połączone w stos z punktu widzenia reszty infrastruktury muszą być widoczne jako jedno urządzenie, czyli muszą tworzyć jedno logiczne urządzenie zarządzane z jednej linii komend. Porty służące do połączenia w stos muszą być niezależne od minimalnej liczby wymaganych portów liniowych, nie mogą także ograniczać możliwości ich rozbudowy. Do przełącznika musi być dołączony kabel służący do połączenia w stos o długości co najmniej 1m.
<b>Obsługa VLAN</b>	Min. 4094 tagi VLAN oraz min. 4094 jednoczesnych sieci VLAN obsługa protokołu QinQ Obsługa protokołu VXLAN

### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

CECHA	OPIS WYMAGAŃ
Tablica MAC	Min. 64000
Tablica Routingu	Min. 10000 (dla IPv4)
Protokoły routingu	Obsługa protokołów routingu: ruting statyczny, RIP v1, RIP v2, RIPng, OSPF, OSPFv3, VRRP, PIM-SM, BGP. Jeżeli do działania któregoś z wymienionych protokołów wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania.
Zasilanie	<ul style="list-style-type: none"><li>• Napięcie zmienne: 230 V, 50 Hz.</li><li>• Dwa wbudowane (wewnętrzne, modułarne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia.</li><li>• Maksymalny pobór mocy urządzenia nie może przekraczać 190W</li></ul>
Warunki środowiskowe	Minimalny zakres temperatury pracy od 0°C do 40°C



## 8.9 Przełącznik serwerowy

CECHA	OPIS WYMAGAŃ
<b>Szybkość przełączania</b>	Minimum 480 Gb/s (na wszystkich portach przełącznika, nie licząc magistrali stackującej)
<b>Przepustowość</b>	Minimum 285 Mpps
<b>Interfejsy sieciowe 10Gb</b>	Przełącznik musi posiadać minimum 16 portów 10G SFP+. Nie dopuszcza się uzyskania portów SFP+ poprzez zastosowanie kabli rozszywających
<b>Interfejsy sieciowe 1Gb</b>	Przełącznik musi mieć możliwość obsługi portów o prędkości 1Gb Ethernet zależnie od wykorzystanej wkładki. Przełącznik musi mieć możliwość obsługi wkładki SFP w porcie SFP+
<b>Rozbudowa</b>	Możliwość rozbudowy o dodatkowe 8 portów SFP+ lub 2 porty QSFP+. Obydwie opcje muszą być dostępne w chwili składania oferty. Dodatkowe porty muszą być w pełni niezależne od portów podstawowych (rozbudowa nie jest wymagana w przypadku, gdy ilość portów w dostarczonym przełączniku jest odpowiednia większa niż wymagane minimum np. 24 porty SFP+ i 2 port QSFP+). Nie dopuszcza się uzyskania portów SFP+ poprzez zastosowanie kabli rozszywających.
<b>Stackowanie</b>	Przełącznik musi posiadać co najmniej 2 dedykowane porty umożliwiające łączenie w stos. Wydajność fizycznych portów stackujących co najmniej 40 Gbps na port. Oprogramowanie przełącznika musi umożliwiać połączenie co najmniej 10 aktywnych urządzeń w stos. Przełączniki połączone w stos z punktu widzenia reszty infrastruktury muszą być widoczne jako jedno urządzenie, czyli muszą tworzyć jedno logiczne urządzenie zarządzane z jednej linii komend. Porty służące do połączenia w stos muszą być niezależne od minimalnej liczby wymaganych portów liniowych, nie mogą także ograniczać możliwości ich rozbudowy. Do przełącznika musi być dołączony kabel służący do połączenia w stos o długości co najmniej 1m.
<b>Obsługa VLAN</b>	Min. 4094 tagi VLAN oraz min. 4094 jednoczesnych sieci VLAN Obsługa protokołu QinQ Obsługa protokołu VXLAN

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

CECHA	OPIS WYMAGAŃ
Tablica MAC	Min. 64000
Tablica Routingu	Min. 10000 (dla IPv4)
Protokoły routingu	Obsługa protokołów rutingu: ruting statyczny, RIP v1, RIP v2, RIPng, OSPF, OSPFv3, VRRP, PIM-SM, BGP. Jeżeli do działania któregoś z wymienionych protokołów wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania.
Warunki środowiskowe	Minimalny zakres temperatury pracy od 0°C do 40°C
Zasilanie	Napięcie zmienne: 230 V, 50 Hz. Dwa wbudowane (wewnętrzne, modułarne) zasilacze AC dla zapewnienia redundancji zasilania, wymieniane podczas pracy urządzenia. Maksymalny pobór mocy urządzenia nie może przekraczać 190W

## 8.10 Firewall w HA i licencje UTM – wspólne dla wszystkich typów firewall

CECHA	OPIS WYMAGAŃ
<b>Wymagania ogólne</b>	<p>Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.</p> <p>System instalowany będzie w formie klastrów HA, wymagane jest by możliwa była konfiguracja minimum klastra active-standby. Przez pojedynczy UTM w zestawieniu ilościowym, rozumie się system złożony z 2 urządzeń fizycznych pracujących w klastrze HA.</p>

**Funkcje  
modułu  
Firewall**

Musi umożliwiać zdefiniowanie co najmniej 15 grup interfejsów (Zone, Alias, itp.).

Musi obsługiwać protokoły dynamicznego routingu: RIP, OSPF i BGP.

Musi obsługiwać policy based routing.

Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPOE) na zewnętrznym interfejsie.

Musi obsługiwać DHCP v6 na zewnętrznym interfejsie.

Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP, jako bridge (transparent mode)).

Musi mieć możliwość obsługi wielu łączy zewnętrznych z opcją balansowania ruchu.

Musi mieć możliwość obsługi łącza zapasowego typu LTE poprzez podłączenie zewnętrznego modemu.

Musi obsługiwać Dynamic DNS.

Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.

Musi obsługiwać translację portów: PAT.

Musi obsługiwać IPSec NAT traversal.

Musi obsługiwać mechanizm policy-based NAT.

Musi obsługiwać VLAN 802.1Q.

Musi zapewniać ochronę przed atakami stosującymi techniki unikania wykrycia, np. fragmentacja pakietów.

Musi zapewniać funkcję serwera DHCP (dla Ipv4 i Ipv6) dla wszystkich interfejsów sieciowych.

Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.

Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.

Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID oraz wewnętrznej bazy użytkowników.

Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.

Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.

Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.

**WOJEWÓDZTWO POMORSKIE**

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



**WOJEWÓDZTWO  
POMORSKIE**

CECHA	OPIS WYMAGAŃ
	<p>Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.</p> <p>Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.</p> <p>Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych – dla najpopularniejszych protokołów.</p> <p>Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: http, https, ftp, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.</p> <p>Musi umożliwiać sterowanie przepustowością w oparciu o następujące parametry: użytkownik, grupa, protokół, polisa, interfejs sieciowy, adres IP, sieć VLAN, aplikacja i kategoria aplikacji.</p> <p>Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.</p>
<p><b>Dostarczony system bezpieczeństwa musi zapewniać</b></p>	<p>Ochronę z wykorzystaniem mechanizmów IPS.</p> <p>Ochronę antywirusową.</p> <p>Możliwość filtrowania URL.</p> <p>Inspekcję ruchu szyfrowanego https.</p> <p>Ochronę przed niechcianą pocztą (AntySPAM).</p> <p>Rozpoznawanie aplikacji w oparciu o analizę ruchu sieciowego a nie wyłącznie nr portu.</p> <p>Filtrowanie treści w oparciu o typy MIME.</p>

CECHA	OPIS WYMAGAŃ
<b>Wymagane funkcje VPN systemu</b>	<p>Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec.</p> <p>W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.</p> <p>Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.</p> <p>Musi wspierać mechanizmy uwierzytelniania: SHA-2, MD5, IKE Pre-Shared Key, certyfikaty.</p> <p>Obsługa Dead Peer Detection (DPD).</p> <p>Wsparcie dla IKEv1 i IKEv2.</p> <p>Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.</p> <p>Wsparcie dla VPN failover (wznawianie połączenia na drugim łączy w przypadku awarii głównego).</p> <p>Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.</p> <p>Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL.</p> <p>Połączenia client-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.</p> <p>Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.</p> <p>Obsługa SSL VPN w trybie portal.</p>

CECHA	OPIS WYMAGAŃ
<b>W ramach filtrowania zawartości URL system musi zapewniać</b>	<p>Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.</p> <p>Baza filtra URL powinna zawierać co najmniej 65 predefiniowanych kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&amp;control, Proxy avoidance, Botnets, Malicious sites, Phishing, Spyware.</p> <p>Możliwość tworzenia białych list wyjątków dla filtrowania zawartości http.</p> <p>W tym umożliwiać blokowanie stron typu:</p> <p>Odpytywanie bazy on-line w czasie rzeczywistym.</p> <p>Możliwość zastosowania komercyjnej bazy kategorii URL lokalnie. Dostarczony system powinien zawierać wszystkie komponenty niezbędne do uruchomienia tej funkcji tak aby można ją było włączyć licencyjnie w późniejszym czasie.</p> <p>Filtrować treści w wielu językach, w tym w języku polskim.</p> <p>Analizę treści dla protokołu https.</p> <p>Wyłączenie inspekcji https dla wybranych kategorii stron www.</p>
<b>W ramach kontroli aplikacyjnej system musi zapewniać</b>	<p>Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.</p> <p>Ilość rozpoznawanych aplikacji: nie mniej niż 1800.</p> <p>W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).</p> <p>Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online, aplikacji społecznościowych typu Facebook/Instagram/Tweeter, Dropbox, GoogleDrive, Facebook Games oraz RemoteControl typu RDP/VNC/TeamViewer/Ammy itp.</p>

CECHA	OPIS WYMAGAŃ
<p><b>W ramach kontroli antywirusowej system musi zapewniać</b></p>	<p>Możliwość uruchomienia co najmniej 2 skanerów antywirusowych lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie.</p> <p>Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.</p> <p>Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.</p> <p>Możliwość uruchomienia silnika skanowania bez sygnaturowego lokalnie lub na zewnętrznym skanerze. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.</p> <p>Możliwość tworzenia wyjątków (biała lista) dla określonych domen.</p> <p>Wykrywanie i blokowanie spyware'u.</p> <p>Skanowanie plików skompresowanych: zip, tar, rar, gzip, 7zip) z wieloma poziomami kompresji.</p> <p>Wsparcie dla głównych protokołów: http, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.</p> <p>Możliwość zablokowania aktywności ransomware uruchomionego na stacjach roboczych i serwerach, który nawiązuje komunikację pomiędzy strefami bezpieczeństwa.</p>
<p><b>W ramach kontroli antyspamowej system musi zapewniać</b></p>	<p>Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.</p> <p>Kwarantannę wiadomości e-mail wskazanych przez moduł Antyspam.</p> <p>Blokowanie spamu w wielu językach w tym w języku polskim.</p> <p>Blokowania spamu opartego na obrazach graficznych.</p>
<p><b>W ramach ochrony przed atakami system musi zapewniać</b></p>	<ol style="list-style-type: none"> <li>1. Automatyczną aktualizację bazy sygnatur IPS.</li> <li>2. Automatyczne blokowanie znanych źródeł ataków.</li> <li>3. Mechanizmy ochrony przed atakami typu DoS i DDoS.</li> <li>4. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.–</li> </ol>



CECHA	OPIS WYMAGAŃ
<p><b>W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać</b></p>	<ol style="list-style-type: none"> <li>1. Analizę behawioralną w oparciu o platformę typu sandbox.</li> <li>2. W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).</li> <li>3. Analizę plików pobieranych przez http/https i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP).</li> <li>4. Ogólne oszacowanie poziomu ryzyka dla analizowanych plików oraz udostępniać informacje o wykrytych działaniach niebezpiecznych.</li> <li>5. Możliwość blokowania poczty zawierającej podejrzane załączniki do czasu zakończenia ich analizy.</li> <li>6. Skuteczność wykrywania malware'u – minimum 98% (potwierdzone zewnętrznymi testami).</li> </ol>
<p><b>W ramach ochrony przed phishingiem system musi zapewniać</b></p>	<ol style="list-style-type: none"> <li>1. Mechanizmy ochrony przed phishingiem.</li> <li>2. Możliwość blokowania dostępu do spreparowanych stron.</li> <li>3. Kontrolę przed phishingiem dla co najmniej: http oraz poczty elektronicznej.</li> <li>4. Notyfikację użytkownika, którego dotyczy zdarzenie – niezależnie od logów i raportów.</li> <li>5. Ochronę przed nadużyciem protokołu DNS.,</li> </ol>
<p><b>Zarządzanie</b></p>	<p>Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.</p> <p>Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.</p> <p>W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).</p> <p>Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji – muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.</p> <p>Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.</p> <p>Komunikacja do systemów logowania i raportowania musi być szyfrowana.</p> <p>W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.</p>

<p><b>Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania</b></p>	<p>Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.</p> <p>Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.</p> <p>Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online</p> <p>Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.</p> <p>Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.</p> <p>System ma posiadać metodę porównywania różnych wersji konfiguracji.</p> <p>System zarządzania musi posiadać graficzną konsolę do zarządzania połączeniami VPN.</p> <p>Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.</p> <p>System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.</p> <p>Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.</p> <p>Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.</p> <p>Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.</p> <p>Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.</p> <p>Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.</p> <p>Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.</p> <p>System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.</p> <p>System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.</p> <p>Powinna być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.</p> <p>System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.</p> <p>System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.</p> <p>Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.</p> <p>Rozwiązanie nie może narzucać ograniczeń co do czasu przechowywania logów.</p>
--	--

CECHA	OPIS WYMAGAŃ
	System musi zapewniać korelację zdarzeń.
<b>Gwarancja i licencje</b>	<p>W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualizacji baz funkcji ochronnych i serwisów. Powinny one obejmować co najmniej:</p> <ul style="list-style-type: none"> <li>Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Kontrola antywirusowa sygnaturowa, Kontrola antywirusowa bez sygnaturowa, Bazy reputacyjne adresów, Rozpoznawanie urządzeń pracujących w sieci, Analiza typu Sandbox, Ochrona przed wyciekiem danych (DLP), Raportowanie podatności na stacjach roboczych, Ochrona przez phishingiem - na okres 5 lat.</li> </ul>
<b>Tryby pracy</b>	<ul style="list-style-type: none"> <li>Możliwość łączenia w klastr Active-Active lub Active-Passive.</li> <li>System realizujący funkcję UTM musi dawać możliwość pracy minimum w jednym z dwóch trybów: Routera z funkcją NAT lub transparentnym</li> </ul>
<b>Zasilanie</b>	Napięcie zmienne: 230 V, 50 Hz.
<b>Redundancja</b>	funkcja łączenia urządzeń w klastry wysokiej dostępności.
<b>Warunki środowiskowe</b>	Minimalna temperatura pracy od 0°C do 45°C
<b>Obudowa</b>	Dostosowana do montażu w szafie stelażowej 19".

## 8.11 Firewall w HA i licencje UTM – Typ A

CECHA	OPIS WYMAGAŃ
<b>Parametry wydajnościowe systemu</b>	<p>Przepustowość Firewall minimum: 18 Gbps.</p> <p>Firewall musi obsługiwać 3500000 jednoczesnych połączeń oraz przyjmować nowe połączenia z wydajnością minimalną 80 tysięcy nowych połączeń na sekundę.</p> <p>W ramach Firewall system musi obsługiwać min.: 300 jednoczesnych sieci VLAN.</p> <p>Element systemu pełniący funkcję Firewall musi dysponować : 8 portami 10/100/1000BaseT</p> <p>Możliwość rozbudowy o co najmniej 4 porty 10Gb SFP+</p> <p>Przepustowość IPSec VPN nie mniejsza niż: 5 Gbps.</p> <p>Obsługa nie mniej niż: 250 tuneli IPSec site-to-site.</p> <p>Obsługa nie mniej niż: 250 tuneli client-to-site.</p> <p>Przepustowość skanowania antywirusowego nie mniejsza niż: 3 Gbps</p> <p>Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 5 Gbps.</p> <p>Przepustowość systemu z włączonymi mechanizmami AV oraz IPS minimum: 3 Gbps.–</p> <p>Możliwość wysyłania logów do zewnętrznego serwera syslog</p>

## 8.12 Firewall w HA i licencje UTM – Typ B

CECHA	OPIS WYMAGAŃ
<b>Parametry wydajnościowe systemu</b>	<p>Przepustowość Firewall minimum: 4,5 Gbps.</p> <p>Firewall musi obsługiwać 2 miliony jednoczesnych połączeń oraz przyjmować nowe połączenia z wydajnością minimalną 20 tysięcy nowych połączeń na sekundę.</p> <p>W ramach Firewall system musi obsługiwać min.: 100 jednoczesnych sieci VLAN.</p> <p>Element systemu pełniący funkcję Firewall musi dysponować : 8 portami 10/100/1000 BaseT.</p> <p>Przepustowość IPSec VPN nie mniejsza niż: 1,5 Gbps.</p> <p>Obsługa nie mniej niż: 50 tuneli IPSec site-to-site.</p> <p>Obsługa nie mniej niż: 50 tuneli client-to-site.</p> <p>Przepustowość skanowania antywirusowego nie mniejsza niż: 2 Gbps</p> <p>Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 2 Gbps.</p> <p>Przepustowość systemu z włączonymi mechanizmami AV oraz IPS minimum: 1,5 Gbps.</p>

## 8.13 Kontroler sieci bezprzewodowej – wymagania wspólne dla Typów A, B i C

CECHA	OPIS WYMAGAŃ
<b>Sprzęt</b>	Kontroler musi zostać dostarczony postaci fizycznego urządzenia (appliance)
<b>Podstawowe funkcje</b>	<p>Centralne zarządzanie wszystkimi dostarczonymi punktami dostępowymi AP w sieci, łącznie z tworzeniem i zarządzaniem konfiguracją oraz aktualizacją oprogramowania. Do kontrolerów muszą być dostarczone licencje w liczbie równej liczbie wymaganych AP, tak by zapewniona była obsługa odpowiedniej liczby AP per PL (jeżeli licencje występują w paczkach po kilka, musi być ich odpowiednia liczba per każde PL)</p> <p>Możliwa współpraca z zewnętrznym systemem uwierzytelniania i kontroli dostępu dla klientów sieci bezprzewodowej</p> <p>Możliwość utworzenia nie mniej niż 16 SSID na jednym punkcie dostępowym.</p>
<b>Parametry sieciowe</b>	<p>Wsparcie dla sieci VLAN w tym również dla konfiguracji typu vlan trunk</p> <p>Wbudowany serwer DHCP</p> <p>Obsługa SNMPv2, SNMPv3</p> <p>Możliwość integracji z zewnętrznymi serwerami autoryzacji i systemami Network Access Control</p>
<b>Współpraca z innymi rozwiązaniami</b>	WEP, TKIP WPA, WPA2, , EAP, PEAP, TLS, EAP-FAST
<b>Metody szyfrowania i kontroli połączeń</b>	<p>Możliwość wykorzystania mieszanego szyfrowania dla określonych SSID (np. WPA/TKIP i WPA2/AES)</p> <p>Obsługa SSL i TLS</p> <p>Typy uwierzytelnienia: IEEE 802.1X (co najmniej EAP, PEAP, EAP-TLS), Captive Portal</p>
	Możliwość wykorzystania nazwy użytkownika, adresu MAC i klucza szyfrowanego do uwierzytelnienia

CECHA	OPIS WYMAGAŃ
<b>Autoryzacja i uwierzytelnianie dostępu użytkowników do sieci</b>	<p>Uwierzytelnienie oraz autoryzacja musi być możliwa przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających.</p> <p>Kontroler musi wspierać co najmniej serwery AAA Radius.</p>
<b>Transmisja danych</b>	<p>Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe</p>
<b>Zarządzanie pasem radiowym</b>	<p>Stałe monitorowanie pasma oraz usług</p> <p>Rozkład ruchu pomiędzy różnymi punktami dostępowymi bazując na ilości użytkowników oraz utylizacji pasma</p> <p>Wykrywanie interferencji oraz miejsc bez pokrycia sygnału</p> <p>Wsparcie dla 802.11h</p> <p>Moduł musi posiadać następujące funkcję:</p> <ul style="list-style-type: none"> <li>• detekcje i identyfikacja lokalizacji obcych punktów dostępowych (rogue AP).</li> <li>• ochronę przed atakami sieciowymi na sieć bezprzewodową</li> </ul>
<b>Interfejsy fizyczne</b>	<p>Interfejs konsoli (RS-232), RJ-45.</p>
<b>Zarządzanie</b>	<p>Zarządzanie kontrolerem musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli</p>

CECHA	OPIS WYMAGAŃ
<b>Licencje</b>	<p>Kontroler musi zostać dostarczony z permanentnymi licencjami do obsługi wymaganej ilości AP dostępowych</p> <p>Wszystkie funkcje muszą być dostępne bez licencji. Jeżeli do działania którejkolwiek z funkcji wymagana jest licencja to należy ją dostarczyć w ramach tego postępowania. Licencja nie może być ograniczona czasowo.</p> <p>Wszystkie wymagane funkcje muszą być dostępne bezpośrednio na kontrolerze – nie dopuszcza się realizację niektórych z wymienionych funkcji poprzez zaoferowanie dodatkowego komponentu w postaci oprogramowania nie będącego częścią kontrolera</p>
<b>Zgodność z normami</b>	<ul style="list-style-type: none"><li>• 55022 Class A IEC/EN 60950</li><li>• CE Marking</li></ul>



## 8.14 Kontroler sieci bezprzewodowej TYP A

CECHA	OPIS WYMAGAŃ
Ilość obsługiwanych AP	<ul style="list-style-type: none"><li>Kontroler jest w stanie obsłużyć minimum 16 punktów dostępowych</li></ul>
Interfejsy	<ul style="list-style-type: none"><li>Minimum 4 x Ethernet 10/100/1000BaseT</li><li>1 x Port USB 2.0 służący do podłączenia zewnętrznego nośnika danych</li><li>1x port konsoli RJ45 lub DB9</li><li>1 x port konsoli USB (niezależny od portu USB 2.0)</li></ul>
Zasilanie	<ul style="list-style-type: none"><li>Maksymalny pobór mocy 120 W</li></ul>
Parametry pracy	<ul style="list-style-type: none"><li>Temperatura pracy od 0°C do 40°C</li><li>Wilgotność nie skondensowana od 10 % do 95%</li><li>Chłodzenie pasywne (bez wentylatorów)</li></ul>
Wydajność	<ul style="list-style-type: none"><li>Obsługa minimum 1024 użytkowników/urządzeń</li><li>Obsługa minimum 4094 VLANów</li></ul>
Inne funkcje	<ul style="list-style-type: none"><li>Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania i sieci VLAN</li><li>Musi być możliwość zdefiniowania co najmniej jednego portalu „captive portal”</li></ul>
Parametry fizyczne	<ul style="list-style-type: none"><li>Waga poniżej 2 Kg</li><li>Możliwość montażu na ścianie lub w szafie RACK (dołączony zestaw montażowy)</li></ul>

## 8.15 Kontroler sieci bezprzewodowej TYP B

CECHA	OPIS WYMAGAŃ
Ilość obsługiwanych AP	<ul style="list-style-type: none"><li>Kontroler jest w stanie obsłużyć minimum 64 punktów dostępowych</li></ul>
Interfejsy	<ul style="list-style-type: none"><li>Minimum 8 x Ethernet 10/100/1000BaseT</li><li>Minimum 4 x 1000BaseX SFP (dopuszcza się porty Combo)</li><li>1 x Port USB 2.0 służący do podłączenia zewnętrznego nośnika danych</li><li>1x port konsoli RJ45</li><li>1 x port konsoli USB (niezależny od portu USB 2.0)</li></ul>
Zasilanie	<ul style="list-style-type: none"><li>Wbudowany zasilacz AC</li><li>Maksymalny pobór mocy 600 W</li></ul>
Parametry pracy	<ul style="list-style-type: none"><li>Temperatura pracy od 5° C do 40 °C</li><li>Wilgotność nie skondensowana od 10 % do 85%</li><li>Szum akustyczny nie większy niż 71dBa</li></ul>
Wydajność	<ul style="list-style-type: none"><li>Obsługa minimum 4096 użytkowników/urządzeń</li><li>Obsługa minimum 4094 VLANów</li></ul>
Inne funkcje	<ul style="list-style-type: none"><li>Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, sieci VLAN i portalu „captive portal”</li></ul>
Parametry fizyczne	<ul style="list-style-type: none"><li>Waga poniżej 15 Kg</li><li>Możliwość montażu w szafie RACK (dołączony zestaw montażowy)</li></ul>

## 8.16 Kontroler sieci bezprzewodowej Typ C

CECHA	OPIS WYMAGAŃ
Ilość obsługiwanych AP	<ul style="list-style-type: none"> <li>Kontroler jest w stanie obsłużyć minimum 256 punktów dostępowych</li> </ul>
Interfejsy	<ul style="list-style-type: none"> <li>Minimum 4 x Ethernet 10/100/1000BaseT</li> <li>Minimum 4 x 1000BaseX SFP (dopuszcza się porty Combo)</li> <li>Minimum 2 x 10GBaseX SFP+ lub SFP28</li> <li>1 x Port USB 2.0 służący do podłączenia zewnętrznego nośnika danych</li> <li>1x port konsoli RJ45</li> <li>1 x port konsoli USB (niezależny od portu USB 2.0)</li> </ul>
Zasilanie	<ul style="list-style-type: none"> <li>Wbudowany zasilacz AC</li> <li>Maksymalny pobór mocy maximum 600 W</li> </ul>
Parametry pracy	<ul style="list-style-type: none"> <li>Temperatura pracy od 5°C do 40°C</li> <li>Wilgotność nie skondensowana od 10 % do 85%</li> <li>Szum akustyczny nie większy niż 71dBa</li> </ul>
Wydajność	<ul style="list-style-type: none"> <li>Obsługa minimum 8192 użytkowników/urządzeń</li> <li>Obsługa minimum 4094 VLANów</li> </ul>
Inne funkcje	<ul style="list-style-type: none"> <li>Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, sieci VLAN i portalu „captive portal”</li> </ul>
Parametry fizyczne	<ul style="list-style-type: none"> <li>Waga poniżej 15 Kg</li> <li>Możliwość montażu w szafie RACK (dołączony zestaw montażowy)</li> </ul>

## 8.17 Access Point

CECHA	OPIS WYMAGAŃ
Rodzaj AP	Punkt dostępowy do montażu wewnątrz budynków, pracujący w dwóch kanałach radiowych jednocześnie (obsługując standardy 802.11an, 802.11bgn, 802.11ac, 802.11ac Wave 2)
	Punkt dostępowy 2x2 MIMO, o wzmacnieniu co najmniej: 3 dBi dla 2.4GHz oraz 5 dBi dla 5GHz
Podstawowe funkcję	Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej dostarczonym przez Wykonawcę w ramach postępowania
	Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID per radio
Parametry sieciowe	Wsparcie dla sieci VLAN
	Każde SSID musi mieć możliwość przypisania niezależnie w sposób statyczny lub dynamiczny do sieci VLAN
	Wbudowany serwer DHCP
	Obsługa protokołów SNMPv1, SNMPv2c, SNMPv3
Specyfikacja radia 802.11a/n/ac	Obsługiwane częstotliwości: <ul style="list-style-type: none"> <li>• 5.150 - 5.250 GHz</li> <li>• 5.250 - 5.350 GHz</li> <li>• 5.470 - 5.725 GHz</li> <li>• 5.725 - 5.825GHz</li> </ul>
	Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM
	Prędkości transmisji: 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a/g, 802.11n MCS0-MCS23 (6,5Mbps do 450Mbps), 802.11ac MCS0 do MCS9, NSS = 1 do 3 (6.5 do 1300 Mbps)
	Obsługa HT, kanały 20, 40 oraz VHT 20/40/80MHz
	Możliwość konfigurowana mocy transmisji przez administratora (zwiększenie/zmniejszenie)
Specyfikacja radia 802.11b/g/n:	Częstotliwość 2,412 - 2,472GHz
	Typy modulacji –BPSK, QPSK,16-QAM, 64-QAM

### WOJEWÓDZTWO POMORSKIE

ul. Okopowa 21/27, 80-810 Gdańsk

tel. 58 32 68 524, faks 58 32 68 526

e-mail: [dc@pomorskie.eu](mailto:dc@pomorskie.eu), [www.pomorskie.eu](http://www.pomorskie.eu)



WOJEWÓDZTWO  
POMORSKIE

CECHA	OPIS WYMAGAŃ
	<p>Prędkości transmisji: 6,9,12,18,24,36,48,54 Mbps dla 802.11g</p> <p>Prędkości od MCS0 do MCS15 (6.5 Mbps do 300 Mbps) dla 802.11n</p> <p>Obsługa kanałów 20 MHz oraz 40MHz</p> <p>Możliwość konfigurowana mocy transmisji przez administratora (zwiększenie/zmniejszenie)</p> <p>Oprogramowanie urządzenia musi mieć wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci</p>
<b>Bezpieczeństwo</b>	Możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS
<b>Uwierzytelnianie dostępu użytkowników do sieci</b>	<p>Na urządzeniu musi być obsługiwane terminowanie sesji radius EAP w nie mniej niż następujących opcjach:</p> <ul style="list-style-type: none"> <li>• EAP-TLS</li> <li>• PEAP-MSCHAPv2</li> <li>• PEAP</li> <li>• TTLS-MSCHAPv2</li> </ul> <p>Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:</p> <ul style="list-style-type: none"> <li>• Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe</li> <li>• Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu</li> <li>• Rozkład ruchu pomiędzy różnymi punktami dostępowym bazując na ilości użytkowników oraz utylizacji pasma</li> <li>• Wsparcie dla 802.11d oraz 802.11h</li> <li>• Obsługa tzw. „Fast Handover” polegająca na automatycznym przełączaniu klientów do punktu dostępowego oferującego najlepszy sygnał</li> </ul>

CECHA	OPIS WYMAGAŃ
Zarządzanie pasem radiowym	Obsługa roamingu klientów w warstwie 2
	Obsługa szybkiego roamingu klientów pomiędzy punktami dostępowymi z wykorzystaniem nie mniej niż standardu 802.11r
	<ul style="list-style-type: none"> <li>• Obsługa detekcji, identyfikacji i lokalizacji obcych punktów dostępowych (rogue AP)</li> </ul>
Zarządzanie	Zarządzanie musi odbywać się poprzez co najmniej następujące metody: interfejs przeglądarki Web (https), linia komend przez SSH i dedykowany port konsoli
Interfejsy fizyczne	1 interfejs 10/100/1000 Base-T PoE z możliwością zasilania przez PoE, standardy 802.3at oraz 802.3af
	1 interfejs 10/100/1000 Base-T (sumarycznie 2 interfejsy 10/100/1000BaseT, co najmniej 1 z PoE)
	Interfejs konsoli (RS-232 lub USB)
	Przycisk/syk umożliwiający przywracanie konfiguracji fabrycznej
Montaż	Urządzenie musi być dostarczone elementem do montażu na suficie podwieszanym, suficie lub na ścianie.
Parametry pracy	<ul style="list-style-type: none"> <li>• Minimalny zakres temperatury pracy od 0°C do 50°C</li> <li>• Wilgotność 10% - 90%</li> </ul>
Zgodność z normami	<ul style="list-style-type: none"> <li>• EN 60950-1</li> <li>• Znak CE</li> </ul>
Obsługiwane standardy	<ul style="list-style-type: none"> <li>• Ethernet IEEE 802.3 / IEEE 802.3u</li> <li>• Wireless IEEE 802.11a/b/g/n/ac wave 2</li> </ul>